EdgeAccess™
Universal Chassis System

CANOGA PERKINS

L351 10/100BASE Media Converter User Manual

NOTICE

Canoga Perkins has prepared this users manual for use by customers and Canoga Perkins personnel as a guide for the proper installation, operation and/or maintenance of Canoga Perkins equipment. The drawings, specifications and information contained in this document are the property of Canoga Perkins and any unauthorized use or disclosure of such drawings, specifications and information is prohibited.

Canoga Perkins reserves the right to change or update the contents of this manual and to change the specifications of its products at any time without prior notification. Every effort has been made to keep the information in this document current and accurate as of the date of publication or revision. However, no guarantee is given or implied that the document is error free or that it is accurate with regard to any specification.

CANOGA PERKINS CORPORATION
20600 Prairie Street
Chatsworth, California 91311-6008
Business Phone: (818) 718-6300
(Monday through Friday 7 a.m. – 5 p.m. Pacific Time)
FAX: (818) 718-6312 (24 hrs.)

Website: www.canoga.com
Email: fiber@canoga.com

EdgeAccess®
Universal Chassis System
L351 10/100BASE Media Converter
User Manual
Model Number L351-UM
Part Number 6912580
Rev. G 06/2010
Software Version 5.4

To see Technical Advisories and Product Release Notes, go to Canoga Perkins' website.

CAUTION!

This product may contain a laser diode emitter operating at a wavelength of 1300 nm - 1600 nm. Use of optical instruments (for example: collimating optics) with this product may increase eye hazard. Use of controls or adjustments or performing procedures other than those specified herein may result in hazardous radiation exposure.

Under normal conditions, the radiation levels emitted by this product are under the Class 1 limits in 21 CFR Chapter 1, Subchapter J.

ATTENTION!

Cet équipement peut avoir une diode laser émettant à des longueurs d'onde allant de 1300nm à 1600nm. L'utilisation d'instruments optiques (par exemple : un collimateur optique) avec cet équipement peut s'avèrer dangereuse pour les yeux. Procéder à des contrôles, des ajustements ou toute procédure autre que celles décrites ci-après peut provoquer une exposition dangereuse à des radiations.

Sous des conditions normales, le niveau des radiations émises par cet équipement est en dessous des limites prescrites dans CFR21, chapitre 1, sous chapitre J.

NOTICE!

This device contains static sensitive components. It should be handled only with proper Electrostatic Discharge (ESD) grounding procedures.

NOTE!

Cet équipement contient des composants sensibles aux décharges électro-statiques. Il doit absolument être manipulé en respectant les règles de mise à la terre afin de prévenir de telles décharges.

Table of Contents

List of Figures

List of Tables

Chapter 1
Overview

The Edge Access L351 Series 10/100BASE Media Converters convert and extend Ethernet media between Local Area Networks (LANs) located up to 120 Km apart.

In addition, the L351 offers Layer 2 statistics, local and remote loopback, remote software upgrade, and remote control and monitoring through the SideBand Management Channel (SBMC).

1.1 L351 Series

The L351 receives and transmits 10/100BASE Ethernet data on single mode or multimode fiber optic cable.

The L351 front panel, shown in Figure 1-1, includes:

- User port: UTP connector
- Extension port: SC connector, simplex or duplex; simplex requires a pair of L351s, one at 1310 nm wavelength and the other at 1550 nm wavelength
- Status LEDs:
  - STA shows L351 status
  - CFG shows configuration and setup status
  - 100 and FDX show status for the User port
  - LNK/RX and TX pairs for the User and Extension ports show that data is received and transmitted

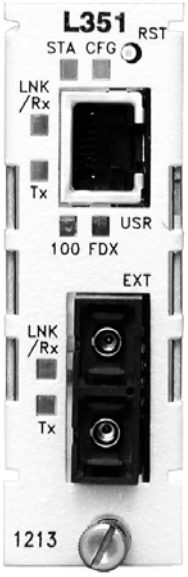

Figure 1-1. The L351

1.2 L351 Hosts

The L351 can be used in a variety of chassis. To install the L351 in a UCS 1000 or UCS 1001 chassis, you must use a Model 1230 Bus Access Module (BAM). However, you can install the L351 directly in a UCS 1002 or Model 1020 or 1030 enclosures.

- The UCS 1000 Chassis can hold up to 15 Model 1230 BAMs with up to two L351s per BAM. This allows a total of 30 L351s per UCS 1000.
- The UCS 1001 Chassis can hold up to two Model 1230 BAMs with up to two L351s per BAM. This allows a total of four L351s per UCS 1001.
- The UCS 1002 Chassis directly hosts up to 14 L351s, or 13 L351s with the optional Domain Management Module (DMM) installed.
- A 1020 or 1030 standalone enclosure holds one L351.

The L351 is hot swappable; it can be inserted or removed at any time without disrupting the data transfer of other modules in the chassis.

Chapter 2
Setup and Installation

This section describes how to set up and install the L351.

Before setting up the L351, make sure the chassis is installed and its Users Manual is available for reference. If the system includes an optional DMM and CIM(s), make sure these are available:

- Serial cable (required to connect the chassis or 1020 enclosure to a VT100 type terminal or PC)
- VT100 type terminal or PC to run the User Interface manager
- The DMM and CIM manuals

2.1 Unpack and Inspect

Unpack and inspect all components. Save the shipping carton and packing materials in case you need to return the equipment to the manufacturer. Appendix A provides information for Return Material Authorization (RMA).

2.2 Set Up the L351

Before inserting the L351, look up the model number to verify that the L351 provides the wavelength and fiber mode type that match its link partner.

For installation in a UCS 1001 or a Model 1030 enclosure, or if you plan to use the Hardware Option Control see Chapter 4, set SW2 and SW3 (see Figure 2-1 and Table 2-1). For more information about the SW2 and SW3 functions, see Chapter 3.

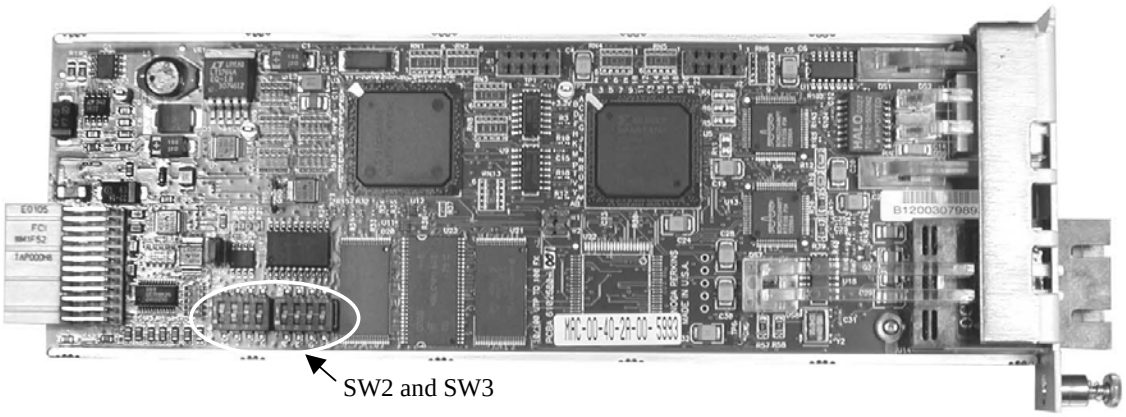

Figure 2-1. SW2 and SW3 Locations

Table 2-1. SW2 and SW3 Functions

Position	Function	On	Off
SW2-1/ 100	User Port 100M Speed	Select 100M speed	Select 10 M speed
SW2-2/A	User Port Auto-Negotiate	Enable automatic data rate and duplex selection	Follow SW2-1 and 2-3 settings
SW2-3/F	User Port Full Duplex	Select full duplex	Select half duplex
SW2-4/N	Not Used	N/A	N/A
SW3-1/S	SBMC	Enable SBMC	Disable SBMC
SW3-2/L	LLF, Extension to User	Enable Link Loss Forwarding (LLF) propagating from Extension Port to User Port	Disable LLF propagating from Extension Port to User Port
SW3-3/U	LLF, User to Extension	Enable LLF propagating from User Port to Extension Port	Disable LLF propagating from User Port to Extension Port
SW3-4/E	Extension Port LLE/RMTF (if SBMC is disabled) or RMTF only (if SBMC is enabled)	Enable LLE for Extension Port (Disables RMTF)	Disable LLE for Extension Port (Enables Remote Fault)

Note: Factory default hardware control setting for User Port Auto-Negotiate is ON. SMBC shipping configuration is disabled.

2.2.1 Install the L351 in a BAM Host

Each BAM can hold up to two L351s. Follow these steps to install the BAM and the L351:

1. Insert a BAM into any available slot of either a 1000 or 1001 chassis. Slide the BAM into the rails and push it firmly into the backplane, then tighten the captive screws. If you encounter resistance, pull the BAM out and check that no connector pins are bent.

2. Insert the L351 into an unused slot in the BAM. Slide the L351 into the rails and push it firmly into the backplane, then tighten the captive screw. If you encounter resistance, pull it out and check that no connector pins are bent.

If you encounter more difficulty, contact Canoga Perkins at (800) 360-6642 for technical assistance.

Note: The L351 and BAM are hot-swappable and can be inserted or removed without disrupting data transfer in other application modules.

2.2.2 Install the L351 in a UCS Model 1002 or Standalone Enclosure

Insert the L351 into an unused slot. Slide the L351 into the rails and push it firmly into the backplane, then tighten the captive screw. If you encounter resistance, pull it out and check that no connector pins are bent. If you encounter more difficulty, contact Canoga Perkins at (800) 360-6642 for technical assistance.

Note: The L351 is hot-swappable and can be inserted or removed without disrupting data transfer in other modules in the chassis.

2.3 Install the Cables

The L351 uses both electrical and fiber optic cables. Electrical UTP cables connect to the User port. Fiber optic cables connect to the Extension port. Dirty optical connectors are a common source of link loss or attenuation problems, especially for single mode fiber (SMF). Clean the connectors before plugging in a cable and whenever there is a significant or unexplained light loss. To prevent contamination, always install protective dust covers on unused fiber optic connectors.

Follow these steps to install the cables:

1. Wipe the ferrule and the end-face surface of the male fiber coupler with a lint-free isopropyl alcohol pad from a fiber cleaning kit.

2. Use canned air to blow out any dust from the female fiber coupler.

Caution: To avoid damaging the fiber end-surface or connector, use extreme care when installing or removing cables.

3. Plug in the optical cables:

   - If you have a single fiber connector (BIDI), plug the cable into a pair of L351s, one at 1310 nm/1470 nm wavelength and the other at 1550 nm wavelength.
   - If you have a duplex connector, use Tx to Rx, and Rx to Tx orientation.

Caution: To protect the Ethernet port from an intrabuilding lightning surge, use a properly grounded shielded cable.

4. Plug the UTP Ethernet cable with RJ-45 connector into the User port on the front of the L351.

5. Label each cable and connector with a signal name and direction.

2.4 Measure Fiber Link Attenuation and Transmit Power

Canoga Perkins recommends that you determine and record link attenuation and transmission power before starting normal link traffic. The attenuation factor and transmission power identify potential problems with links near the lower limit of receiver limitations.

For details on link attenuation and transmission power, see Chapter 5.

Chapter 3
User Operation

This chapter describes the hardware features and functions of the L351.

3.1 L351 Functions

Each L351 requires a host for power. The L351 can function as a non-managed, standalone unit; as a managed, standalone unit; or as a managed unit in a chassis with other application modules.

3.2 Power Up

During the initial power-up sequence, all LEDs light amber. When start-up is complete, the setup and installation are correct, and data is transmitting normally across the link, the STA LED lights green and the LNK/Rx and Tx LEDs for both ports light green or blink green when they transmit or receive data. See Table 3-1.

3.3 Front Panel LEDs

The LEDs on the front panel show the system and port conditions. The STA LED shows the link condition. The LNK/Rx and Tx LEDs show the conditions on the User and Extension Ports and can be used as an aid when troubleshooting a fault. Table 3-1 shows the LED states for various conditions.

In the UCS 1000 and 1001, a BAM holds up to two L351s. On the BAM, the STA LED lights green if either L351 is operating normally. If both L351s are in error conditions, the BAM STA LED lights amber.

3.4 Alarms

The L351 can generate Major and Minor Alarms.

- In the UCS 1000 and 1002, these alarms are forwarded over the backplane to the CIM and appear on the Major (MAJ) and Minor (MIN) CIM LEDs and then are forwarded to the DMM for monitoring and transfer to the Network Manager as traps.
- In the UCS 1001, the alarm outputs are forwarded to the chassis motherboard.

For details about the Alarm Output Configuration, Alarm Log, and Trap Configuration screens, see Chapter 4.

Table 3-1. L351 LEDs

LED	Status	Description
STA	Off	No power
	Green	Normal operation
	Amber	System self-test
	Amber blinking	Downloading file
	Red	Major alarm
CFG	Off	SBMC is disabled
	Green	SBMC is enabled
	Amber	System self-test
	Red	Configuration error
LNK/Rx (User Port)	Off	No link
	Green	Link Established
	Green blinking	Receiving activity
	Amber	System self-test
TX (User Port)	Off	No transmission activity
	Green	Transmission activity
	Amber	Port in standby mode or system self-test
	Red	Transmission disabled due to LLF or port disabled
100	Off	10 M data rate
	Green	100 M data rate
FDX	Off	Half duplex mode
	Green	Full duplex mode
LNK/Rx (Extension Port)	Off	No link
	Green	Link Established
	Green blinking	Receiving activity
	Amber	System self-test
	Red	Receiving Remote Fault
Tx (Extension Port)	Off	No transmission activity
	Green blinking	Transmission activity
	Amber	Port in standby mode or system self-test
	Red	Transmission disabled due to LLF

3.4.1 Remote Fault

If the Extension port Rx loses the signal, it sends a Remote Fault (RMTF) signal from its Tx, the Rx LED is off, and an alarm flags the link loss on the Extension port. When the Extension port receives a Remote Fault signal, the Rx LED lights red and an alarm flags the remote side optical link failure. Both local and remote link partners must be configured to the same RMTF enable/disable setting. RMTF complies with the IEEE802.3u Remote Fault standard.

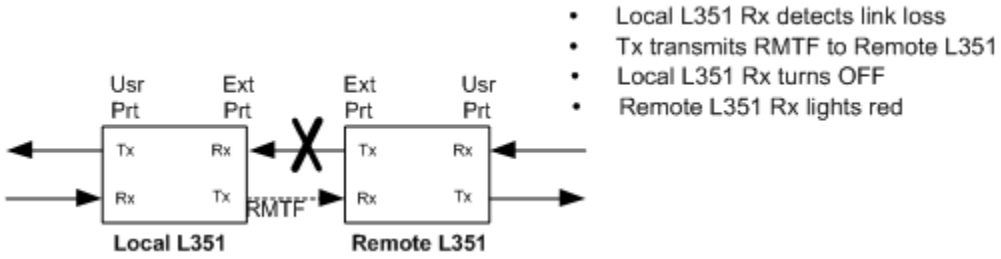

Figure 3-1. Remote Fault Signal

3.4.2 Link Loss Forwarding

When Link Loss Forwarding (LLF) is enabled, a fault on one side of the L351 propagates to the other side to notify that device and stops signal transmission (brings down the link). See Figure 3-2. Set the LLF propagation to User to Extension, Extension to User, or both directions. Set this in the User Interface or at SW3-2 (L) and SW3-3 (U). For details on setting SW3, see Chapter 2.

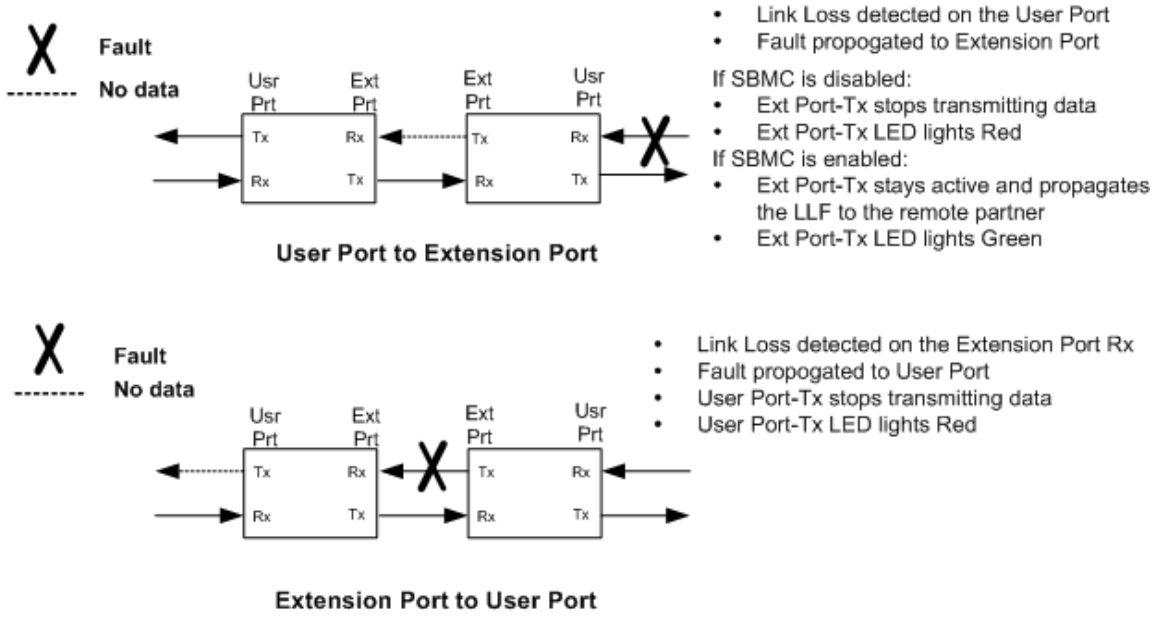

Figure 3-2. Link Loss Forwarding Propagation

3.4.3 Link Loss Echo

Caution: ***To avoid a lockup condition, do not set LLE at both the local and remote ends of the link.***

Link Loss Echo (LLE) propagates a link loss to the device connected to the L351 Extension Port. See Figure 3-3. If a link loss is detected on the Extension Port Rx, the Extension Port Tx is disabled, echoing the fault back to the source. LLE configures the L351 to not send data until it receives data. Set this in the User Interface or at SW3-4 (E). For details on setting SW3, see Chapter 2.

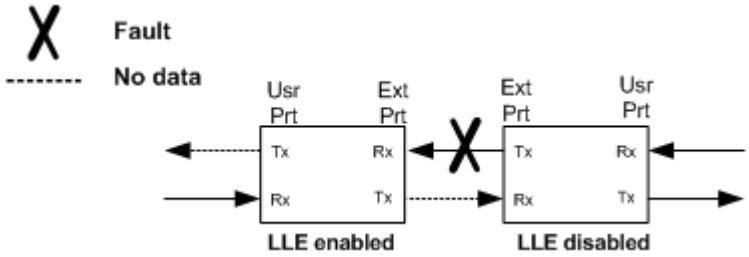

Figure 3-3. Link Loss Echo Detection

Note: LLE is available only when SBMC is disabled; use LLF when you enable SBMC.

3.4.4 Loopback

The L351 supports four loopback modes that you can set at the local site for both the Local and Remote L351s. These modes loop the data through either the physical layer (PHY) on the User side or the FPGA. For details on setting loopback in software, see Chapter 4.

- Local-Local mode loops the electrical data that the Local L351 receives on the local User Port Rx through the FPGA to the User Port Tx. The data is not sent out the Extension Port Tx and incoming data on the Extension Port Rx is ignored. See Figure 3-4. To set this mode at the Diagnostics screen, set the Loopback State for the Local module to Local.

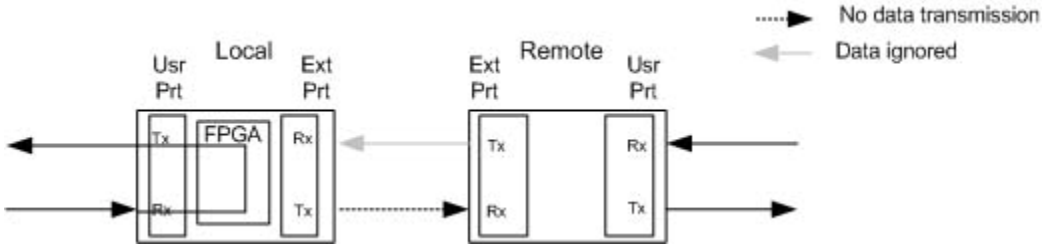

Figure 3-4. Local-Local Loopback Mode

- Local-Remote mode loops the optical data that the Remote L351 receives on the Extension Port Rx through the User PHY to the Extension Port Tx. The data is not sent out the remote User Port Tx and incoming data on the remote User Port Rx is ignored. See Figure 3-5. To set this mode at the Diagnostics screen, set the Loopback State for the Local module to Remote.

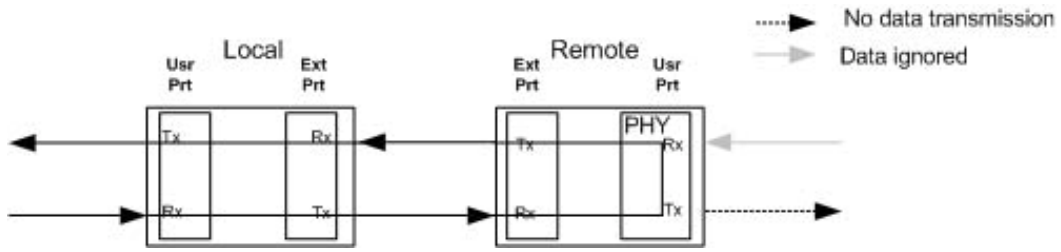

Figure 3-5. Local-Remote Loopback Mode

- Remote-Local mode loops the electrical data that the Remote L351 receives on the User Port Rx through the FPGA to the User Port Tx. The data is not sent out the remote Extension Port Tx and incoming data on the remote Extension Port Rx is ignored. See Figure 3-4. To set this mode, at the Diagnostics screen, set the Loopback State for the Remote module to Local.

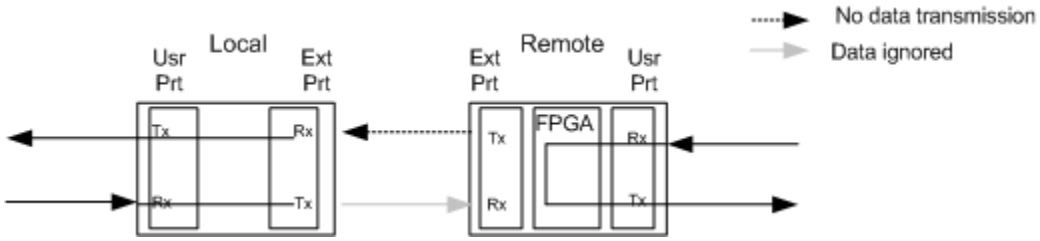

Figure 3-6. Remote-Local Loopback Mode

- Remote-Remote mode loops the optical data that the Local L351 receives on the Extension Port Rx through the Local User PHY to the Extension Port Tx. The data is not sent out the local User Port Tx and incoming data on the local User Port Rx is ignored. See Figure 3-5. To set this mode, at the Diagnostics screen, set the Loopback State for the Remote module to Remote.

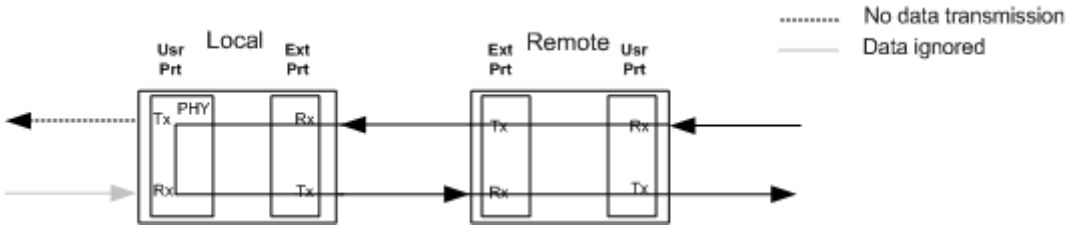

Figure 3-7. Remote-Remote Loopback Mode

For loopback, the L351 uses a unique MAC address that is listed on the Diagnostics screen as Loop Test MAC Address; for details about using the software and accessing the Diagnostics screen, see Chapter 4. In loopback mode, the L351 filters the incoming packets to identify the test packets through the MAC address. You can set two diagnostics options if you want to alter the data during loopback, Swap MAC Address at Loopback Point, which swaps the test MAC address with the source MAC address, and Recalculate CRC at Loopback Point. The test packets are returned to the source according to the selected mode.

Chapter 4
Management - VT100

If the L351 is installed in a UCS1000 or UCS1002 chassis, or if the system includes a DMM and a CIM, or if the L351 is in a Model 1020 enclosure, you can manage the system through VT100 Terminal Emulation, which is accessible by a Telnet session, HyperTerminal or similar terminal emulation software, a standard SNMP network manager, and CanogaView.

4.1 VT100 Terminal Emulation

Connect the VT100 terminal emulation session to the DMM used in the UCS 1000 or 1002 chassis or to the BAM or Model 1020 enclosure. You cannot manage an L351 in a Model 1030 enclosure.

For details on the DMM, see the *Model 1500 Domain Management Module User Manual* (for UCS 1000) or *Model 1502 Domain Management Module User Manual* (for UCS 1002).

Setting up the VT100 session depends on which connection, serial port or Ethernet, you have available for access to the VT100 management program. Canoga Perkins suggests that you use HyperTerminal for your first session. You must set up TCP/IP for the DMM before you can use Telnet; for details, see the manual for the DMM.

4.2 PC Configuration for Terminal Operation

These steps briefly describe how to set up your PC for a terminal connection. For details on using Windows, see your Windows documentation.

1. Turn on your PC.
2. Select Start>All Programs>Accessories, Communications, and click HyperTerminal.
3. In the Connection Description dialog box, enter a name for the connection to the system, select an icon, and click OK.
4. In the Connect To dialog box, select the COM1 port from the Connect Using dropdown menu and click OK.
5. In the COM1 Properties dialog box, ensure the following settings:
    - Bits per second: 19200 bps
    - Data bits: 8
    - Parity: None
    - Stop bits: 1
    - Flow control: None
6. Click Apply, and then click OK. The HyperTerminal will connect to the system.
7. Select the Properties button from the HyperTerminal window or dialog box.
8. In the L351 HyperTerminal window or dialog box, select the Settings tab.
9. Select VT100 from the Emulation dropdown menu and click OK.

4.3 Management User Interface

The Management User Interface for the L351 provides screens for setup, monitoring, and diagnostics. You can access the screens directly by connecting to the serial port of the BAM, the Model 1020, the DMM in the chassis, or by establishing a Telnet session with the DMM. For details, see the *Model 1500 Domain Management Module User Manual* (for UCS 1000) or *Model 1502 Domain Management Module User Manual* (for UCS 1002).

These sections discuss the screens for the L351, using a Telnet session for access.

4.3.1 General Screen Format

A typical screen, shown in Figure 4, includes standard descriptions and reference designations. Use this and other screens to configure the system, set operational parameters, and verify the system status. All screens use a common method for navigation.

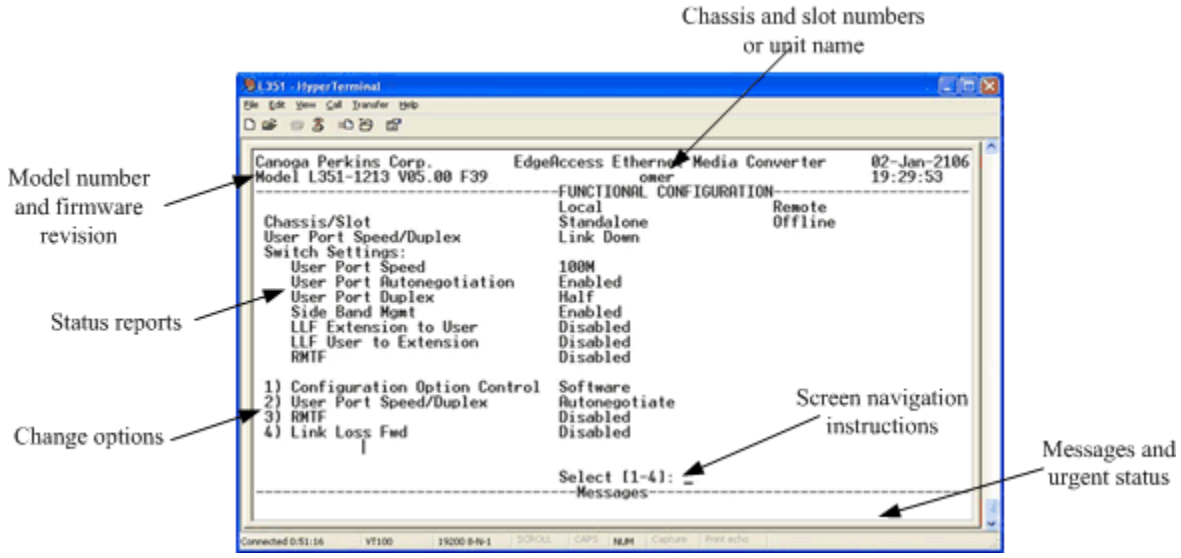

Figure 4-1. General Screen Format

Not all screens and menus provide options that you can change. Some menu items reach screens that only report status, such as revision numbers, module type, or alarms. On other screens, you can move through and select options, and enter data.

Use these keys to navigate the screens:

- Space bar - When a menu item is highlighted, press <Space> to cycle through all options for that item.
- Tab - To move the highlight to the next column to the right.
- Enter - To select the highlighted option for a menu item.
- Escape - To return to the previous screen.

4.3.2 User Interface Organization

The user interface consists of selectable, nested screens, available in the following order.

The paragraphs that follow describe each of these screens in detail.

Main Menu

1) System Configuration

1) Hardware Information

- SFP Information
- Remote Information

2) Functional Configuration

1) Configuration Option Control
2) User Port Speed/Duplex
3) RMTF
4) Link Loss Fwd
5) Remote Configuration

3) Trap Configuration

1) Master Trap Control
2) Local User Port Link Traps
3) Remote User Port Link Traps
4) Extension Port Link Traps
5) Remote Fault Received Traps
6) Link Loss Forwarding Traps
7) Link Loss Echo Traps
8) Cold Start Traps
9) Authentication Traps
10) Side Band Mgmt Channel Traps
11) Diagnostics Traps
12) Configuration Traps
13) Power/Fan/Temperature Traps
14) SFP Traps
15) Alarm Input Traps

4) Alarm Output Configuration

1) Factory Defaults
2) Link Down Alarm
3) RMTF Alarm
4) LLF Alarm
5) Configuration Alarm
6) Power/Fan/Temperature Alarm
7) SBMC Loss Alarm
8) Power-On Self Test Alarm
9) SFP Transmitter Warning
10) SFP Transmitter Failure

5) System Information

1) System Name
2) Contact
3) Location
4) Customer
5) Information
6) Circuits
7) Service Code
8) Date-in-Service
9) Date-Out-of-Service
10) Equipment Type
11) Equipment Code
12) Vendor
13) CLEI
14) Mfg Date
15) Unit

6) IP/SNMP Agent Configuration

1) Management IP Configuration
2) Host Table
3) Trap Table
4) Remote Auxiliary IP Configuration

7) Security Configuration

PASSWORD CONFIGURATION

1) Minimum Length
2) Minimum Alpha Characters
3) Minimum Numeric Characters
4) Minimum Punctuation Characters
5) Maximum Consecutive Character Types
6) Maximum Same Character
7) Allow username in password
8) Password Expiration Time
9) Password Reuse Count

LOCKOUT/LOGOUT CONFIGURATION

10) Lockout After Failed Attempts
11) Lockout Type
    Lockout time
12) Display Lockout Message
13) Lockout Message
14) Lockout Craft Port
15) Inactivity Logout time (mins)

8) Account Configuration

admin

suppervisor

operator

observer

9) Radius Client Configuration

1) Radius Client Mode
2) Radius Server IP Address
3) Radius Server IP Address

10) SNTP Client Configuration

1) Sntp Client UTC Offset (hours)
2) Sntp Client Observe DST
3) Sntp Client Sync Interval (minutes)
4) Sntp Server IP Address
5) Sntp Server IP Address

11) SYSLOG Client Configuration

1. Syslog Server IP Address
   Syslog Server Port
   Syslog Server Mask
2. Syslog Server IP Address
   Syslog Server Port
   Syslog Server Mask

2) Diagnostics

1) Loopback Setup
2) Remote Latency/Jitter Test
3) Remote Connectivity Loss Detection

3) Link Status

4) System Alarms

5) Layer 2 Statistics

6) System Log

7) Utilities

1) Set Date and Time
2) Reset Configuration To Default
3) Reset Remote Configuration To Default
4) Remote Craft Port: Enabled
5) Modem/Slip/PPP Baud Rate
6) Modem Initialization String
7) PING Generation
8) Static ARP Table
9) Dynamic ARP Table

8. Software Upgrade

1) Software Reset
2) Swap Bank & Reset
3) Get New File with TFTP
4) Copy Software from Source Unit to Destination Unit

9. Manage Logged In Users

10. Logout

4.3.3 Login Menu

The first screen is the Login Menu. If this is your initial setup and no password has been set, type **admin** at the Login Username prompt and press <Enter>, then type **admin** at the prompt for the password and press <Enter>. Otherwise, type your username and press <Enter>, then type your password and press <Enter>.

4.3.4 DMM Main Menu

If you are using a DMM, after you log in, the Main Menu for the DMM appears. This is the main management screen for the DMM. For details on all menu options, see the *Model 1500 Domain Management Module Users Manual* (for UCS 1000) or *Model 1502 Domain Management Module Users Manual* (for UCS 1002). From this screen, you can access the L351 by either of two methods.

To reach the L351 directly, follow these steps:

a. Type 4, Manage or access a specific Module, and press <Enter>.

b. Type the slot and chassis numbers with a slash, such as `1/4` for chassis 1, slot 4, and then press <Enter>.

c. At the Module Menu, type 4, Access User Interface, then press <Enter> to reach the Main Menu screen for the L351.

To reach the chassis, and then select the L351, follow these steps:

a. Type 3, Manage or access a specific Chassis, and press <Enter>, press <Space> to cycle between the chassis in the domain, and then press <Enter> to select the chassis.

b. At the Chassis Management screen, press <Space> to cycle to the slot number for the L351, then press <Enter> to reach the Main Menu screen for the L351.

Note: In a UCS 1000 chassis, slots in the BAM appear as A and B for the slot that the BAM is in.

4.4 L351 Main Menu

The Main Menu (see Figure 4-2) appears after you log in. It provides access to all functions for the L351: setup, diagnostics, and reports. The Logout option is available only when the L351 is in a 1020 standalone enclosure.

```
                    ---------MAIN MENU----------

1) System Configuration
2) Diagnostics
3) Link Status
4) System Alarms
5) Layer 2 Statistics
6) System Log
7) Utilities
8) Software Upgrade
9) Manage Logged In Users
10) Logout


                                Select [1-10]:
```

Figure 4-2. L351 Main Menu

4.5 System Configuration Menu

The System Configuration menu provides access to most configuration options for the L351. To access the System Configuration menu, Figure 4-3 and Table 4-1 and follow these steps:

1. From the Main Menu, type 1, System Configuration, and press <Enter>. The System Configuration menu appears.

2. To return to the Main Menu, press <Esc>.

```
                  ----------SYSTEM CONFIGURATION----------
1) Hardware Information
2) Functional Configuration
3) Trap Configuration
4) Alarm Output Configuration
5) System Information
6) IP/SNMP Agent Configuration
7) Security Configuration
8) Account Configuration
9) Radius Client Configuration
10) SNTP Client Configuration
11) SYSLOG Client Configuration

                               Select [1-11]:

                ----------------Messages-----------------
```

Figure 4-3. System Configuration Menu

Table 4-1.System Configuration Option Definitions

Configuration Option	Description
1) Hardware	Shows the chassis slot, CLIM type, revision and serial numbers, fan, chassis temperature status, and Power Supply options; does not offer configurable options
2) Functional	Shows converter functions; you can update the configuration and set the options
3) Trap	Shows the trap configuration; you can enable/disable traps to the Network Manager
4) Alarm Output	Shows the alarm configuration; you can set each alarm parameter to Major, Minor or Off
5) System Information	Shows general information about the L351
6) IP/SNMP Agent	Shows the SNMP parameters if a Network Manager is in use and the L351 is in a Model 1020; you can set options.
7) Security	Shows parameters for passwords, lockout, and logout; you can set options
8) Account	Shows user account information; you can set options
9) Radius Client	Shows parameters for client mode and server settings; you can set options
10) SNTP Client	Shows parameters for SNTP client and server settings; you can set options
11) SYSLOG Client	Shows parameters for SYSLOG server settings; you can set options

4.5.1 Hardware Information Screen

The Hardware Information screen shows various statuses, including the CLIM type, with model and revision numbers, and the power supply fan status. In addition, it shows information about the types of User and Extension ports. To view the Hardware Information screen, see Figure 4-4 and follow these steps:

1. From the Main Menu, type `1`, System Information, and press <Enter>. The System Configuration menu appears.

2. From the System Configuration menu type `1`, Hardware Configuration, and press <Enter> (see Figure 4-5).

Note: For SFP information, press Ctrl+ S.

The View Additional Information About Remote Device Hardware option only applies if the remote unit is a Canoga Perkins device.

3. To view additional information about the remote device hardware, press <Tab> (see Figure 4-6).

4. To return to the System Configuration menu, press <Esc>.

```
--------------------------HARDWARE INFORMATION-------------------------
                                --
                            Local                     Remote

Chassis Type              5U UCS 1000               2U UCS 1002
Chassis/Slot              4/3B                      2/5

CLIM Type                 L351-1213                 L351-1313
User Port                 10/100 BASE-TX UTP RJ48   10/100 BASE-TX UTP
RJ48
Extension Port            100 1310 SM SC 10d        100 1310 SM SC 1-d
Serial Number             20030590295               20030590296
Hardware Rev.             A1                        A1

Power Supply Pri          DC Non Iso                AC 120/240
Power Supply Sec          AC 120/240                DC

Fan Status                OK                        OK
Chassis Temperature       N/A                       OK


       Press CTRL-S for SFP info, ESC to return to previous screen
```

Figure 4-4. Hardware Information Screen

```
----------------------------SFP INFORMATION--------------------------
                          Local                       Remote 9145

User Port:
  Model Number            N/A                         N/A
  Wavelength              N/A                         N/A
  Connector Type          N/A                         N/A
  Data Rate               N/A                         N/A
  Maximum Link Length     N/A                         N/A
  Maximum Loss Budget     N/A                         N/A

Extension Port:
  Model Number            N/A                         N/A
  Wavelength              N/A                         N/A
  Connector Type          N/A                         N/A
  Data Rate               N/A                         N/A
  Maximum Link Length     N/A                         N/A
  Maximum Loss Budget     N/A                         N/A

                Press ESC to return to previous screen

------------------------------Messages-----------------------------
```

Figure 4-5. SFP Information Screen with 9145 as the Remote Partner

```
-------------------------REMOTE HARDWARE INFORMATION----------------

Model Number              9145-4
Hardware Rev.             CC
Serial Number             20050592421

User Port Model Number    9400-330
User Port Description     10/100/1000 UTP
User Port Hardware Rev.   DA
User Port Serial Number   20050820608

Ext Port Model Number     9400-648
Ext Port Description      100M XD 1310/SM/26dB/SC
Ext Port Hardware Rev.    CA
Ext Port Serial Number    20050124407

Power Supply              AC 120/240

     Press CTRL-S for SFP info, TAB for local info, ESC to return

------------------------------Messages-----------------------------
```

Figure 4-6. Remote Hardware Information Screen

4.5.2 Functional Configuration Screen

The Functional Configuration report and menu provides information about the hardware, with options to set software control. You can view the options for the Remote module, you can set options for both the Local and remote L351 module. For details about how RMTF, LLE, and LLF interact, see Section 3.4. Two reported hardware switch functions depend on the type of module:

1. An L351 with a UTP User port ignores the LLE User settings.

2. An L351 with a fiber User port ignores the User Speed/Duplex settings.

In addition, a system that supports 1000 BASE UTP ports allows only one port set to Master; all others must be set to Slave.

To access the Functional Configuration screen, follow these steps (see Figure 4-7 and Table 4-2):

1. From the Main Menu, type 1, System Configuration, and press <Enter>. The System Configuration menu appears.

2. From the System Configuration menu type 2, Functional Configuration, and press <Enter>.

3. At the Functional Configuration screen, type the number for an item and press <Enter>, then press <Space> to cycle through the options and press <Enter> to select an option for the local or remote L351.

4. To return to the System Configuration menu, press <Esc>.

```
-----------------------------FUNCTIONAL CONFIGURATION-----------------
                                Local                   Remote 9145
Chassis/Slot                    Standalone
User Port Speed/Duplex          Link Down               Link Down
Switch Settings:
   User Port Speed              100M
   User Port Autonegotiation    Enabled
   User Port Duplex             Full
   Side Band Mgmt               Enabled
   LLF Extension to User        Enabled
   LLF User to Extension        Enabled
   RMTF                         Disabled

1) Configuration Option Control  Software
2) User Port Speed/Duplex        Autonegotiate          100M/Full
3) RMTF                          Disabled               Disabled
4) Link Loss Fwd                 Disabled               Disabled
5) Remote Configuration

                            Select [1-5]:
-------------------------------Messages--------------------------------
```

Figure 4-7. Functional Configuration Screen

Table 4-2. Functional Configuration Option Definitions

Menu Item	Description
1) Configuration Option Control	Set the L351 to follow settings in software and ignore SW2 and SW3 settings
2) User Port Speed/Duplex	Set the User Port to specific data rate and duplex options, to automatic rate and duplexing, or disable it
3) RMTF	Enable or disable RMTF if SBMC is enabled or RMTF/LLE if SBMC is disabled
4) Link Loss Fwd	Enable or disable LLF
5) Remote Configuration	Set the software settings on the remote end of the L351

```
-----------------------------REMOTE CONFIGURATION---------------------

                              1) Functional Configuration
                              2) VLAN Configuration
                              3) VLAN ID Translation Table
                              4) P-Bit Translation Table
                              5) Port Filters
                              6) Local Configuration

                             Select [1-6]:

-------------------------------Messages-------------------------------
```

Figure 4-8. Remote Configuration Menu

```
-------------------------REMOTE FUNCTIONAL CONFIGURATION-------------
User Port Speed/Duplex           Link Down

Ext Port Speed/Duplex            100M/Full

1) User Port Setting             100M/Full
2) Ext Port Setting              100M/Full
3) RMTF                          Disabled
4) Link Loss Fwd                 Disabled
5) Flow Control                  Disabled
6) Maximum Frame Size            10000
7) Sideband Management           Enabled

                             Select [1-7]:

-------------------------------Messages-------------------------------
```

Figure 4-9. Remote Functional Configuration Screen

```
  -------------------------REMOTE VLAN CONFIGURATION------------------

                                    User Port   Ext Port
 1)  Drop Untagged Packets?            No          No
 2)  Drop Packets with VLAN Tag
     not matching VLAN Tag A?          No          No
 3)  Remove outermost VLAN Tag?        No          No
 4)  Add VLAN Tag B to Untagged
     Packets only?                     No          No
 5)  Add VLAN Tag C to Tagged
     Packets only?                     No          No
 6)  Add VLAN Tag C to Tagged
     Packets only using P-Bits
     of outermost VLAN tag?            No          No
 7)  Tag A VLAN ID (0 - 4095)           0           0
 8)  Tag B VLAN ID (0 - 4095)           0           0
           Priority (0 - 7)             0           0
 9)  Tag C VLAN ID (0 - 4095)           0           0
           Priority (0 - 7)             0           0
                               Select [1-9]:
  -----------------------------Messages-----------------------------
```

Figure 4-10. Remote VLAN Configuration Screen

```
 ---------------------REMOTE VLAN ID TRANSLATION TABLE-----------------

        User Port          Ext Port
    In VLAN  Out VLAN  Out VLAN  In VLAN
    -------  --------  --------  -------
 1)     0         0         0        0
 2)     0         0         0        0
 3)     0         0         0        0
 4)     0         0         0        0
 5)     0         0         0        0
 6)     0         0         0        0
 7)     0         0         0        0
 8)     0         0         0        0
 9) Enable VLAN
    Translation?  No                 No
                               Select [1-9]:

 -------------------------------Messages-------------------------------
```

Figure 4-11. Remote VLAN Tag Translation Table Screen

```
----------------------REMOTE P-BIT TRANSLATION TABLE-----------------

                                  User Port   Ext Port

1) Incoming P-Bit 0 translated to     0          0
2) Incoming P-Bit 1 translated to     1          1
3) Incoming P-Bit 2 translated to     2          2
4) Incoming P-Bit 3 translated to     3          3
5) Incoming P-Bit 4 translated to     4          4
6) Incoming P-Bit 5 translated to     5          5
7) Incoming P-Bit 6 translated to     6          6
8) Incoming P-Bit 7 translated to     7          7

9) P-Bit Translation Enabled?         No         No

                             Select [1-9]:

-------------------------------Messages--------------------------------
```

Figure 4-12. Remote P-Bit Translation Table Screen

```
      --------------------REMOTE PORT FILTERS--------------------

1) PVST+BPDU Filter                     Disabled
2) MAC Address Filter                   Disabled
3) Test Network Filter                  Disabled
4) OAM BPDUs Filter                     Disabled
5) UDLD Filter                          Disabled
6) Management VLAN Filter               Disabled

                             Select [1-6]:

      --------------------------Messages-------------------------
```

Figure 4-13. Remote Port Filters Table Screen

4.5.3 Trap Configuration

Traps are messages to alert network management about conditions. The DMM logs the traps and the DMM or Model 1020 transmits them by SNMP to the network manager. At the Trap Configuration screen, enable or disable traps individually or use the Master Trap Control to enable or disable all traps. See Figure 4-14. To configure traps, follow these steps:

1. From the Main Menu, type `1`, System Configuration, and press <Enter>. The System Configuration menu appears.

2. From the System Configuration menu type 3, Trap Configuration, and press <Enter>.

3. At the Trap Configuration menu, type the number for a trap and press <Enter>.

Note: Master Trap Control enables or disables all traps. The factory default is Log Only.

4. Press <Space> to cycle to Enabled, Log Only, Both Log And Send, or Disabled, then press <Enter>.

5. To return to the System Configuration menu, press <Esc>.

```
------------------------------TRAP CONFIGURATION----------------------

     1) Master Trap Control                        Log Only

     2) Local User Port Link Traps                 Both Log And Send
     3) Remote User Port Link Traps                Both Log And Send
     4) Extension Port Link Traps                  Both Log And Send
     5) Remote Fault Received Traps                Both Log And Send
     6) Link Loss Forwarding Traps                 Both Log And Send
     7) Link Loss Echo Traps                       Both Log And Send
     8) Cold Start Traps                           Both Log And Send
     9) Authentication Traps                       Both Log And Send
    10) Side Band Mgmt Channel Traps               Both Log And Send
    11) Diagnostics Traps                          Both Log And Send
    12) Configuration Traps                        Both Log And Send
    13) Power/Fan/Temperature Traps                Both Log And Send
    14) SFP Traps                                  Both Log And Send
    15) Alarm Input Traps                          Both Log And Send

                            Select [1-15]:

-------------------------------Messages--------------------------------
```

Figure 4-14. Trap Configuration Screen

4.5.4 Alarm Output Configuration

Use the Alarm Output Configuration screen to set any or all alarms to Major, Minor, or Off. See Figure 4-15 and Table 4-3. To configure alarms, follow these steps:

1. From the Main Menu type 3, Alarm Output Configuration, and press <Enter>. The Alarm Output Configuration screen appears.

2. Type the number for the alarm you want to set and press <Enter>.

3. Press <Space> to cycle to Major, Minor, or Off, and press <Enter>.

```
-------------------------ALARM OUTPUT CONFIGURATION-----------------
      1)  Factory Defaults

      2)  Link Down Alarm                          Minor
      3)  RMTF Alarm                               Major
      4)  LLF Alarm                                Major
      5)  Configuration Alarm                      Off
      6)  Power/Fan/Temperature Alarm              Minor
      7)  SBMC Loss Alarm                          Major
      8)  Power-On Self Test Alarm                 Major
      9)  SFP Transmitter Warning                  Minor
      10) SFP Transmitter Failure                  Major


                            Select [1-10]:

------------------------------Messages------------------------------
```

Figure 4-15. Alarm Output Configuration Screen

Table 4-3. Alarm Output Definitions

Alarm	Description
2) Link Down	Loss of Signal (electrical)/Composite Loss of Signal (optical); one or both received signals fail; default is Off
3) RMTF	Remote fault received; default is Off
4) LLF	Link loss forwarded to module; default if Off
5) Configuration	Setup errors, including mismatches with other modems; default is Off
6) Power/Fan/Temperature	Power is low or fan is off; default is Minor
7) SBMC Loss	SideBand management signal lost; default is Off
8) Power-On Self Test	Modem failed when power was turned on; default is Off
9) SFP Transmitter Warning	
10) SFP Transmitter Failure	

Note: You must enable the Alarm Output item on the System Status & Configuration screen for these settings to take effect.

4.5.5 System Information Screen

The System Information menu provides options to enter general information about this module in the system. To access the System Information screen, see Figure 4-16 and follow these steps:

1. From the System Configuration menu type 5, System Information, and press <Enter>.

2. At the System Information screen, type the number for an item and press <Enter>, then follow the prompts to type in your information.

3. To return to the System Configuration menu, press <Esc>.

```
 ------------------SYSTEM INFORMATION - LOCAL UNIT--------------------

 1. System Name         : omer
 2. Contact             :
 3. Location            :
 4. Customer            :
 5. Information         :
                        :
 6. Circuits            :
                        :
 7. Service Code        :
 8. Date-in-Service     :
 9. Date-Out-of-Service :
10. Equipment Type      :
11. Equipment Code      :
12. Vendor              : Canoga Perkins
13. CLEI                :
14. Mfg Date            : 05/01/2003

15. Unit                : Local

                             Select [1-15]:

 -------------------------------Messages-------------------------------
```

Figure 4-16. System Information Screen

4.5.6 IP/SNMP Agent Configuration

If the L351 is in a Model 1020, use the IP/SNMP Agent Configuration screen to view and set up the SNMP parameters. To view SNMP parameters, follow these steps:

1. At the System Configuration menu type 6, IP/SNMP Agent Configuration, and press <Enter>. The IP/SNMP Agent Configuration screen appears (see Figure 4-17 and Table 4-4).

```
--------------------IP/SNMP AGENT CONFIGURATION--------------------

             1) Management IP Configuration
             2) Host Table
             3) Trap Table
             4) Remote Auxiliary IP Configuration

                          Select [1-4]:

------------------------------Messages------------------------------
```

Figure 4-17. IP/SNMP Agent Configuration Screen

Table 4-4. SNMP Configuration Parameters Description

Item	Description
1) Management IP Configuration	Access the IP Configuration Management Screen
2) Host Table	Access the Host Table screen (for standalone enclosure, only)
3) Trap Table	Access the Trap Table screen (for standalone enclosure, only)
4) Remote Auxiliary IP Configuration	Access the Remote Auxiliary IP Configuration Management Screen

2. Type 1 to access the IP Configuration Management screen, which will allow you to modify the configuration settings shown in Figure 4-17 and described in Table 4-5.

```
     -------------------------MANAGEMENT IP CONFIGURATION----------------
                               Local                  Remote 9145
MAC Address                    00 40 2A 00 58 2D      00 40 2A 00 B3 E2
Management Port                DOWN                   UP
1)  Manager IP Address         172.016.085.055        172.016.085.075
    Subnet Mask                255.255.000.000        255.255.000.000
    Default Gateway            172.016.001.001        172.016.001.001
2)  SLIP/PPP IP Address        000.000.000.000        000.000.000.000
3)  Serial Port Config         VT100                  VT100
4)  BOOTP                      Disabled
5)  Telnet Security            Disabled               Disabled
6)  Test IP Address                                   172.016.085.013
    Test Subnet Mask                                  255.255.000.000
7)  Inband Management Port                            Both Ports
8)  Management VLAN                                   Disabled
9)  Management VLAN Number                            1
                               Select [1-9]:
     ------------------------------Messages------------------------------
```

Figure 4-18. ManagementIP Configuration Screen .

Table 4-5. SNMP Configuration Parameters Description

Item	Description
1) Ethernet IP Address Subnet Mask Default Gateway	Enter the IP address for access through the Ethernet network, the mask that sets the network ID part of the IP address, and the address of the network node that connects to another network
2) SLIP/PPP IP Address	Enter the IP address for access through SLIP or PPP
3) Serial Port Config	Set the type of serial port connection: VT100, SLIP, or PPP
4) BOOTP	Enable this if the module needs to obtain its IP address from a BOOTP server; when the unit has an IP address, disable BOOTP
5) Telnet Security	Enables or disables checking if Telnet host is listed in the host table. Default is disabled, which allows access to all hosts
6) Test IP Address Test Subnet Mask	The Test IP address is not available with the N525.
7) Inband Management Port	Set the port that will receive management packets; can be Ext. only, User only, Both ports, or No Management
8) Management VLAN	Enable or disable the Management VLAN
9) Management VLAN Number	Set the number for the VLAN; range is 0-4095

The SNMP agent allows access to up to 24 Host IP addresses listed in the Host Table. Set up the Host informzation for the L351 on the Host Table screen (see Figure 4-18).

1. Type 2 to access the Host Access Table screen.

2. To add a host, type 1 and press <Enter>, then follow the prompts at the bottom of the screen to enter values for these parameters:

    a. Managing Host IP

    b. IP Mask Size

    c. Telnet Access

    d. FTP Access

    e. SNMP Access

    f. SNMP Protocol

    g. V1/V2c Read Community

    h. V1/V2c Write Community

    i. V1/V2c Access Level

3. To delete a host, type 2 and press <Enter>. Use the space bar to move down the Host Access list, press <Enter> to delete a highlighted entry. Press <Esc> to return to the Host Access Table screen.

4. To return to the IP/SNMP Configuration menu, press <Esc>.

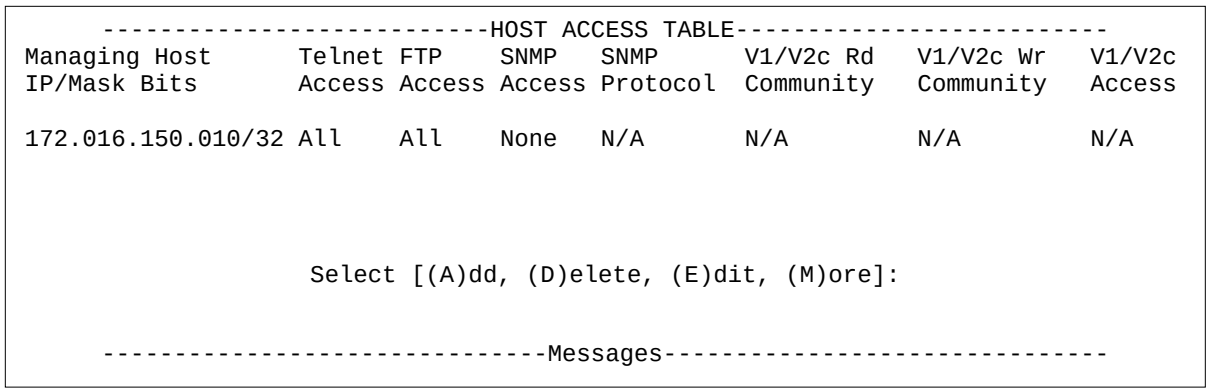

Figure 4-18. Host Access Table Screen

The Trap/Notification Destination Table lists information about, and options to set up, hosts to receive notification of traps and alarms. To access the Trap/Notification Destination Table screen, see Figure 4-19 and follow these steps:

1. From the IP/SNMP Configuration menu type 3 and press <Enter>.

2. At the Trap/Notification Destination Table screen, type 1 to edit a host or 2 to add a host at the Edit Notification Destination Entry screen, or type 3 to remove a host.

3. To return to the IP/SNMP Configuration menu, press <Esc>.

Note: To add or edit a host entry, follow the prompts on the notification destination entry screen.

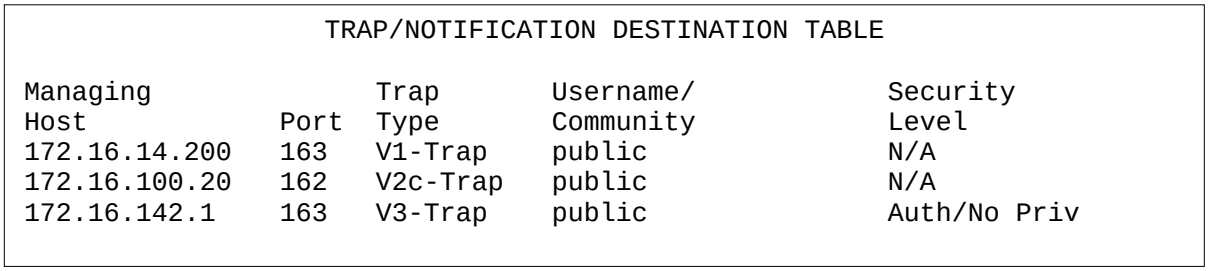

Figure 4-19. Trap/Notification Destination Table Screen

The Aux IP can be placed on any subnet and assigned any valid VLAN ID. By using the Inband Auxiliary Port setting, the user can choose whether the entity is isolated to the User Port only, to the Extension Port only, or if it presents itself on both ports simultaneously. The user will also be able to shut off the entity by setting the Inband Auxiliary Port setting to No Ports Allowed.

1. From the IP/SNMP Configuration menu type 4 and press <Enter>.

2. At the Trap Remote Auxiliary IP Configuration screen, type 1 to add an IP address and/or subnet mask, 2 to choose an Inband port, 3, to enable or disable VLAN tagging, and 4 to assign a VLAN ID number, and then follow the prompts at the bottom of the screen.

3. To return to the IP/SNMP Agent Configuration menu, press <Esc>.

4. To return to the System Configuration menu, press <Esc>.

```
      --------------REMOTE AUXILIARY IP CONFIGURATION-------------

1)  Auxiliary IP Address         000.000.000.000
     Auxiliary Subnet Mask        255.255.255.000
 2)  Inband Auxiliary Port        Both Ports
 3)  Auxiliary VLAN Tagging       Disabled
 4)  Auxiliary VLAN Number        0


                              Select [1-4]:

      --------------------------Messages--------------------------
```

Figure 4-20. Remote Auxiliary IP Configuration screen

4.5.5 Security Configuration

The Security Configuration menu provides options to set values for general parameters for passwords, lockout, and logout. To access the Security Configuration screen, see Figure 4-21 and Table 4-6 and follow these steps:

1. From the System Configuration menu type 6, Security Configuration, and press <Enter>.

2. At the Security Configuration screen, type the number for an item and press <Enter>, then press <Space> to cycle through the options and press <Enter> to select an option.

3. To return to the System Configuration menu, press <Esc>.

```
                        SECURITY CONFIGURATION

   PASSWORD CONFIGURATION
 1. Minimum Length                     :  0
 2. Minimum Alpha Characters           :  0
 3. Minimum Numeric Characters         :  0
 4. Minimum Punctuation Characters     :  0
 5. Maximum Consecutive Character Types :  0
 6. Maximum Same Character             :  0
 7. Allow username in password         :  Disabled
 8. Password Expiration Time           :  0
 9. Password Reuse Count               :  0
   LOCKOUT/LOGOUT CONFIGURATION
10. Lockout After Failed Attempts      :  0
11. Lockout Type                       :  Hard
    Lockout time                       :  0
12. Display Lockout Message            :  Disabled
13. Lockout Message                    :  Account has been locked out
14. Lockout Craft Port                 :  Disabled
15. Inactivity Logout time (mins)      :  0
```

Figure 4-21. Security Configuration Screen

Table 4-6. Security Configuration Option Definitions

Menu Item	Description
1. Minimum Length 2. Minimum Alpha Characters 3. Minimum Numeric Characters 4. Minimum Punctuation Characters 5. Maximum Consecutive Character Types 6. Maximum Same Character	Define characteristics of passwords; the range for all fields is from 0 through 15
7. Allow username in password	Enable or disable the username appearing as or within the password
8. Password Expiration Time	Set how often in days, 1 through 365, that the passwords must be reset; 0 = disabled
9. Password Reuse Count	Set whether the password must be changed or can be used again immediately. Values are 0 to 8. 0 means the new password can be the same. 1 to 8 specify how many times the password must expire before a specific password can be used again.
10. Lockout After Failed Attempts	Set how many times, from 1 to 10, that a user can try to log in before a lockout; 0 = disabled
11. Lockout Type Lockout time	Set the type of lockout: Hard requires another user with admin access to unlock the account on the User Accounts screen; Timed requires that the user wait for Lockout time before trying again; Lockout time is from 0 (none) to 30 minutes
12. Display Lockout Message 13. Lockout Message	Enable or disable and set the message, up to 30 characters, that appears at lockout
14. Lockout Craft Port	Disable access to the serial port to prevent any unauthorized access; to re-enable the craft port, run a Telnet session
15. Inactivity Logout time (mins)	Set the time, between 1 and 30 minutes, before automatic log-out with no activity; 0 = disabled

4.5.6 Account Configuration Screen

The Account Configuration screen provides options to set values for parameters for specific users (see Figure 4-21, Figure 4-22, and Table 4-7) To access the Security Configuration screen, follow these steps:

1. From the System Configuration menu type 7, Account Configuration, and press <Enter>.
2. To add a user, type A, or to edit an existing user, type E, and press <Enter>.
3. On the Edit User Account screen, type the Username, then follow the prompts at the bottom of the screen to enter values, or press <Space> to cycle through options for the effected parameters.
3. To delete a user, type 2, then follow the prompts to select the user name and confirm the choice; the User Accounts screen reappears.
4. To return to the System Configuration menu, press <Esc>.

```
 -------------------------ACCOUNT CONFIGURATION-----------------------
            Account   Access         Access
Locked
Username    State     From           Level       Description         Out

admin       Enabled   UI/SNMPv3      Supervisor  Default Account
No
sup         Enabled   UI/SNMPv3      Supervisor
No
ope         Enabled   UI/SNMPv3      Operator
No
obs         Enabled   UI/SNMPv3      Observer
No
```

Figure 4-21. Account Configuration Screen

```
 ----------------------------EDIT USER ACCOUNT-----------------------

    Username                      :
 1. Account State                 :
 2. Access From                   :
 3. Access Level                  :
 4. Description                   :
 5. UI Password                   :
 6. UI Password Expires           :
    UI Password Expires in (days) :
 7. Allow UI Lockout Of User      :
 8. Allow UI Logout Of User       :
 9. UI Login Locked State         :
10. SNMPv3 Authentication Protocol:
11. SNMPv3 Authentication Password:
    SNMPv3 Authentication Key     :
12. SNMPv3 Privacy Protocol       :
13. SNMPv3 Privacy Password       :
    SNMPv3 Privacy Key            :

        Enter the username [10 characters maximum]


 -----------------------------Messages-------------------------------
```

Figure 4-22. Edit User Account Screen

Table 4-7. User Parameters

Menu Item	Description
1. Account State	enabled or disabled
2. Access From	**UI** - indicates access through Telnet, Console, SSH, FTP, or SFTP, and requires additional parameter setup **SNMPv3** - enhances security and requires additional parameter setup **UI/SNMPv3**
3. Access level	Supervisor Operator Observer
4. Description (Optional)	Up to 17 characters
5. UI Password	Password that allows access through Telnet, Console, SSH, FTP, or SFTP; 8 to 15 characters
6. UI Password Expires UI Password Expires in (days)	Yes or No 0 (never) to 365
7. Allow UI Lockout of User	Yes or No; can disable access for this user after excessive failed attempts to log in
8. Allow UI Logout of User	Yes or No; can automatically log user out after excessive inactivity
9. UI Logout Locked State	Shows current state as Locked, Unlocked, Logged out, or Logged in
10. SNMPv3 Authentication Protocol	MD5, SHA, or None; sets how to authenticate the user
11. SNMPv3 Authentication Password SNMPv3 Authentication Key	Password that generates the authentication key for the user if the authentication protocol is MD5 or SHA; 8 to 15 characters. Shows the key that authenticates the user for MD5 or SHA Authentication Protocol; this is generated automatically for the Authentication Password, but can be changed if the user's host uses a different Authentication Key generation algorithm; 16 Hex characters for MD5 protocol or 20 Hex characters for SHA protocol.
12. SNMPv3 Privacy Protocol	DES or None; sets the protocol for encryption
13. SNMPv3 Privacy Password SNMPv3 Privacy Key	Password that generates the encryption key for the user if the privacy protocol is DES; 8 to 15 characters Shows the key that encrypts messages for DES Privacy Protocol; this is generated automatically for the Privacy Password, but can be changed if the user's host uses a different Privacy Key generation algorithm; 16 Hex characters

4.5.8 Radius Client Screen

Use the Radius Client Configuration Menu to set up communications with the Radius Server to enable Radius Authentication of users at login. To access the Radius Client Configuration Menu, follow these steps:

1. From the System Configuration Menu, type 6 and press <Enter>. The Radius Client Configuration Menu appears (see Figure 4-23).
2. At the prompt, type 1 to set the mode. Type 2 to configure access to the primary Radius server or type 3 to configure access to the alternate Radius server, and then follow the prompts at the bottom of the screen.
3. To return to the System Configuration Menu, press <Esc>.

```
  --------------------RADIUS CLIENT CONFIGURATION----------------------
1. Radius Client Mode                : None
2. Radius Server IP Address          : 0.0.0.0
   Radius Server Shared Secret       :
   Radius Server Retries             : 3
   Radius Server Timeout             : 5
   Radius Server Priority            : 1
3. Radius Server IP Address          : 0.0.0.0
   Radius Server Shared Secret       :
   Radius Server Retries             : 3
   Radius Server Timeout             : 5
   Radius Server Priority            : 1



                              Select [1-3]:
  -------------------------------Messages-------------------------------
```

Figure 4-23. Radius Client Screen

Table 4-8. Radius Client Configuration Option Definitions

Menu Item	Description
Radius Client Mode	Radius then Local Local then Radius None
`Radius Server IP Address`	Sets the address for the Radius Server. An Address 0.0.0.0 indicates no server
`Radius Server Shared Secret`	Must match the Shared Secret set on the Radius Server
`Radius Server Retries`	How many times the L351 tries to authenticate the user before trying the Secondary Server or giving up. Range is 0 to 10
`Radius Server Timeout`	How long, in seconds, between unsuccessful attempts. Range is 1 to 30
`Radius Server Priority`	Sets which server to contact first; Range is 1 (highest priority) to 255 lowest priority) Should priority get set the same for two servers, the L351 will alternate tries between the servers

4.5.9 SNTP Client Configuration Screen

The L351 can be set up to synchronize the system date and time to an SNTP server. When the L351 contacts the SNTP server to synchronize the time, the event appears in the System Log, whether or not the SNTP server responds. If you choose to not use SNTP to maintain the date and time, or do not have access to the Internet or an SNTP server, see paragraph 4.10, Utilities, to manually set the date and time. To set up synchronization with SNTP, follow these steps:

1. At the System Configuration Menu, type 7, SNTP Client Configuration and press <Enter>.

2. At the SNTP Client Configuration screen, type the number for a parameter and press <Enter>, then follow the prompts at the bottom of the screen. When you are done setting that parameter, press <Enter> to return to the SNTP Client Configuration screen.

3. When you have completed configuring the SNTP parameters, press <Esc> to return to the System Configuration Screen.

```
--------------------SNTP CLIENT CONFIGURATION-------------------------

1. Sntp Client UTC Offset (hours)     : 0
2. Sntp Client Observe DST            : Disabled
   Sntp Client DST Starts At          : 01/01/1970 00:00
   Sntp Client DST Ends at            : 01/01/1970 00:00
3. Sntp Client Sync Interval (minutes): 5

4. Sntp Server IP Address             : 0.0.0.0
   Sntp Server Retries                : 3
   Sntp Server Timeout (seconds)      : 5
   Sntp Server Priority               : 1
5. Sntp Server IP Address             : 0.0.0.0
   Sntp Server Retries                : 3
   Sntp Server Timeout (seconds)      : 5
   Sntp Server Priority               : 1



                             Select [1-5]:
--------------------------------Messages--------------------------------
```

Figure 4-24. SNTP Client Configuration Screen

Table 4-9. SNTP Client Configuration Option Definitions

Menu Item	Description
1. Sntp Client UTP Offset	Set the difference, in hours, between this L351 and Coordinated Universal Time (UTC), which is similar to Greenwich Mean Time (GMT); Range is -12 to 12
2. Sntp Client Observe DST	Enables/Disables Daylight Savings Time (Summer Time)
Sntp Client DST Starts At	Sets the date and time DST starts
Sntp Client DST Ends at	Sets the date and time DST starts and ends
3. Sntp Client Sync Interval	Sets how often, in minutes, that the L351 tries to synchronize its time to the SNTP server; Range is 0 (attempt to synchronize at bootup, only) to 1440 (once daily)
4. Sntp Server IP Address	Sets the address for the main SNTP server. 0.0.0.0 indicates no server
Sntp Server Retries	Sets how many times the L351 tries to synchronize before trying the alternate server or giving up. Range is 0 to 10
Sntp Server Timeout	Wait period between unsuccessful attempts. Range is 1 to 30
Sntp Server Priority	Set which server to contact first. Range is 1 to 255 with 1 the highest priority and 255 the lowest. If the priority is the same for the two servers, the L351 alternates tries between the servers
5. Sntp Server IP Address	Sets the address for the alternate SNTP server. 0.0.0.0 indicates no server
Sntp Server Retries	Sets how many times the L351 tries to synchronize before returning to the main server or giving up. Range is 0 to 10
Sntp Server Timeout	Wait period between unsuccessful attempts. Range is 1 to 30
Sntp Server Priority	Set which server to contact first. Range is 1 to 255 with 1 the highest priority and 255 the lowest. If the priority is the same for the two servers, the L351 alternates tries between the servers

4.5.10 Syslog Client Configuration

You can configure and display two server destinations for Syslog messages. In addition to setting the host address and port, you can set the server mask for the notification. To access and update the Syslog Client Configuration, follow these steps:

1. From the System Configuration Menu type 11, Syslog Client Configuration, and press <Enter>.

2. To enter a new Syslog Server or to edit an existing entry, select Syslog Server 1 or Syslog Server 2 and press <Enter>. Enter the values for the Server as described in Table 4-10.

3. To return to the System Configuration Screen, press <Esc>.

4. To return to the Main Menu, press <Esc>.

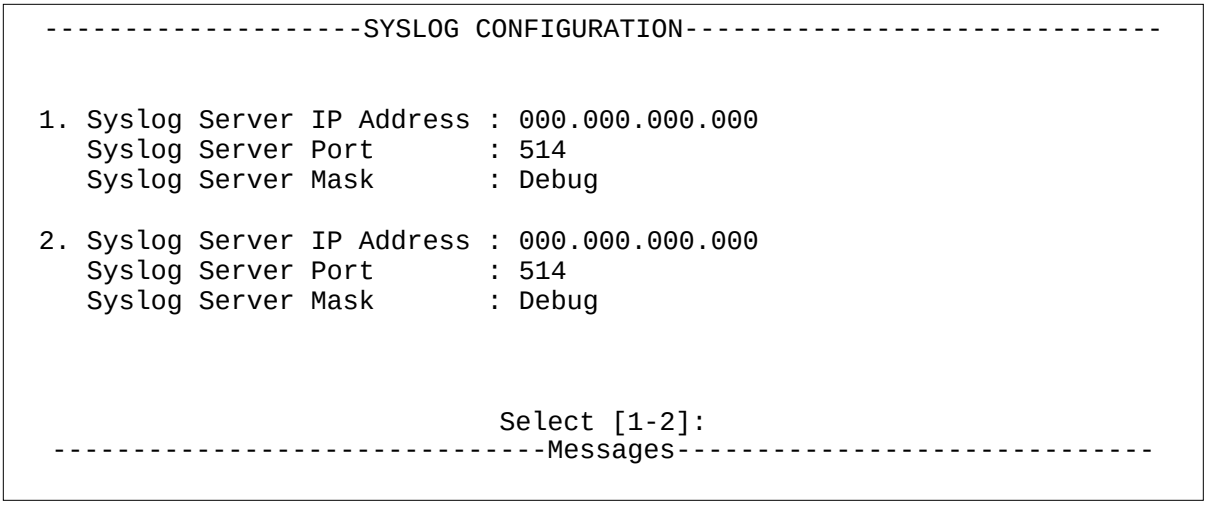

Figure 4-25. SYSLOG Client Configuration Screen

Table 4-10. SYSLOG Client Configuration Option Definitions

Menu Item	Description
1. Syslog Server IP Address	Enter the IP address for the primary Syslog Server None
Syslog Server Port	Enter the UDP Port number used by the Syslog Server
Syslog Server Mask	Sets the Syslog Message Mask. Pressing <Space> cycles through the options. Options are Debug, Emergency, Alert, Critical, Error, Warning, Notice and Informational
2. Syslog Server IP Address	Enter the IP address for the secondary Syslog Server
Syslog Server Port	Enter the UDP Port number used by the Syslog Server, 1-65535
Syslog Server Mask	This sets the Syslog Message Mask. Pressing <Space> cycles through the options. Options are Debug, Emergency, Alert, Critical, Error, Warning, Notice and Informational

4.6 Diagnostics Menu

Use the Diagnostics menu for troubleshooting the L351. You can view current loopback conditions and set up loopback. See Figure 4-26. For details about using loopback, see Chapter 3. To use the Diagnostics, follow these steps:

1. From the Main Menu, type 2, Diagnostics, and press <Enter>. The Diagnostics menu appears.

2. Type the number for the test option you want, and press <Enter>.

3. When you finish running diagnostic tests, press <Esc> to return to the Main Menu.

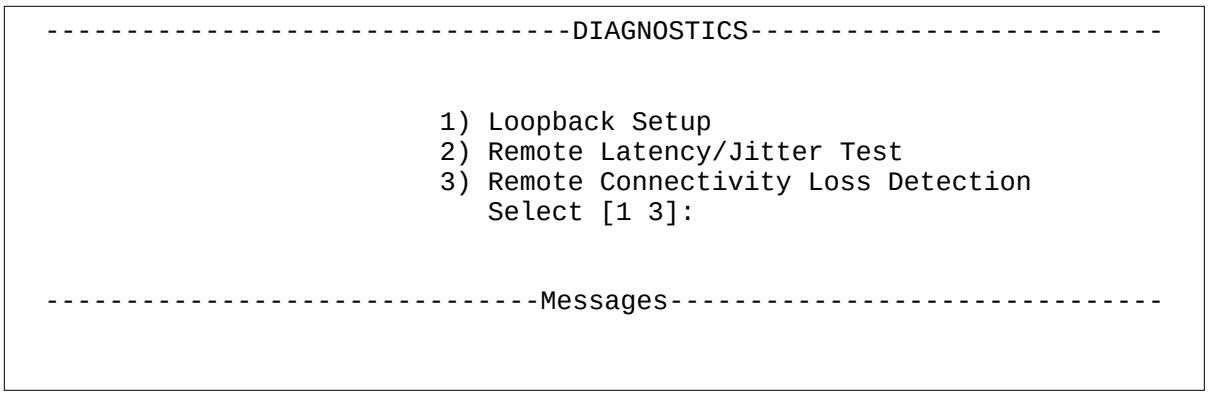

Figure 4-26. Diagnostics Menu

4.6.1 Loopback Setup

Use the Loopback Setup report and menu to view current loopback conditions and set up loopback for troubleshooting the L351. See Figure 4-27 and Table 4-11. For details about using loopback, see Chapter 3. To run a loopback test, follow these steps:

1. From the Diagnostics menu, type `1`, Loopback Setup, and press <Enter>. The Loopback Setup screen appears.

2. Type the number for the loopback option you want to set, press <Tab> to highlight the Remote column if needed, press <Space> to cycle through the options, and press <Enter>.

3. When you finish running Loopback, press <Esc> to return to the Diagnostics menu.

```
   -------------------------------LOOPBACK SETUP-------------------------
                                 Local                      Remote 9145
 Chassis/Slot                    Standalone

 Loopback Switch Setting:        Norm

 Loop Test MAC Address:          00 40 2A 80 58 2D          00 40 2A 80 B3 E2

 1) Loopback Option Control      Software
 2) Loopback State               Disabled                   Disabled
 3) Swap MAC Address
    at Loopback Point?           No                         No
 4) Recalculate CRC
    at Loopback Point?           No                         No


                                Select [1-4]:
-------------------------------Messages--------------------------------
```

Figure 4-27. Loopback Setup Screen

Table 4-11. Diagnostics Screen Definitions

Selection	Description
Loopback Switch Setting	Shows hardware setting only when in a Model 1020; Local, Remote, or Normal
Loop Test MAC Address	Shows unique MAC address for destination of loopback packets
1) Loopback Option Control	Set to Hardware (option for Model 1020 only) or Software
2) Loopback State	Set to Local, Remote, or Clear All Loopbacks
3) Swap MAC Address at Loopback Point?	Set to Yes or No; use to run loopback packets through a switch
4) Recalculate CRC at Loopback Point?	Set to Yes or No; use to run loopback packets through a switch

4.6.1 Remote Latency/Jitter Test

Use the Remote Latency/Jitter Test report and menu to set up test conditions and view test results for troubleshooting the L351 and its link partner. See Figure 4-28. To test latency and jitter, follow these steps:

1. From the Diagnostics menu, type 2, Remote Latency/Jitter Test, and press <Enter>. The Latency/Jitter Test screen appears.
2. Type the number for the test parameter option you want to set, type the value, and press <Enter>.
3. Type 8 to start the test or type 9 to end the test.
4. When you finish running the Remote Latency/Jitter test, press <Esc> to return to the Diagnostics screen.

```
--------------------------REMOTE LATENCY/JITTER TEST----------------

Test IP Addr/VLAN  0.0.0.0/0              Round Trip Packets   0
Test Duration      00:00                  Dropped Packets      0
Minimum Latency (ms)  0.000000            Minimum Jitter (ms)  0.000000
Average Latency (ms)  0.000000            Average Jitter (ms)  0.000000
Maximum Latency (ms)  0.000000            Maximum Jitter (ms)  0.000000

(1) To IP Addr   0.0.0.0                  (5) DF Bit           Clear
(2) From IP Addr Auto Selection           (6) DSCP Precedence  Best Effort
(3) Test VLAN            0                    Drop Probability Not Used
(4) Test Packets per sec  1               (7) Test Packet Priority (0-7) 0

            (8) Test Duration min:sec (0=forever)  0
            (9) Min Test Payload Size (40 - 1954)  40
           (10) Max Test Payload Size (40 - 1954)  40
           (11) Test Packet Timeout sec (1 - 10)   3
           (12) Start Remote Test
           (13) Stop Remote Test

                              Select [1-13]:

------------------------------Messages------------------------------
```

Figure 4-28. Latency/Jitter Test Screen

4.6.2 Remote Connectivity Loss Detection

The Connectivity Loss Detection (CLD) feature enables you to detect loss of connectivity between two N525s in a point-to-point circuit, and to detect undesired link performance. It is possible to remotely configure N525 CLD parameters using the SideBand management channel from an L351. See the diagram below.

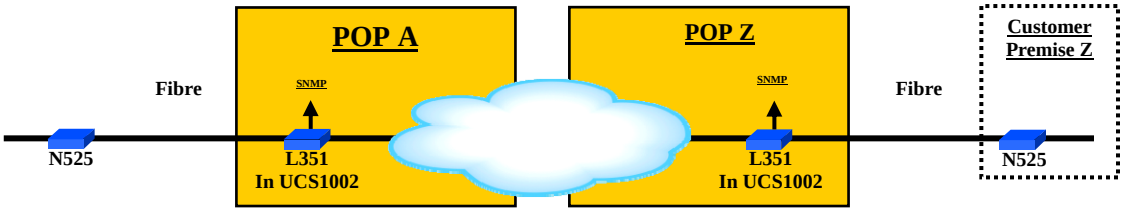

Figure 4-29. N525 to N525 Connectivity Loss Detection

In conjunction with CLD you can use Connection Loss Forwarding (CLF), which will shut down the User port on an N525 if there is a loss of connectivity between the N525 Extension ports. CLD and CLF are disabled by default.

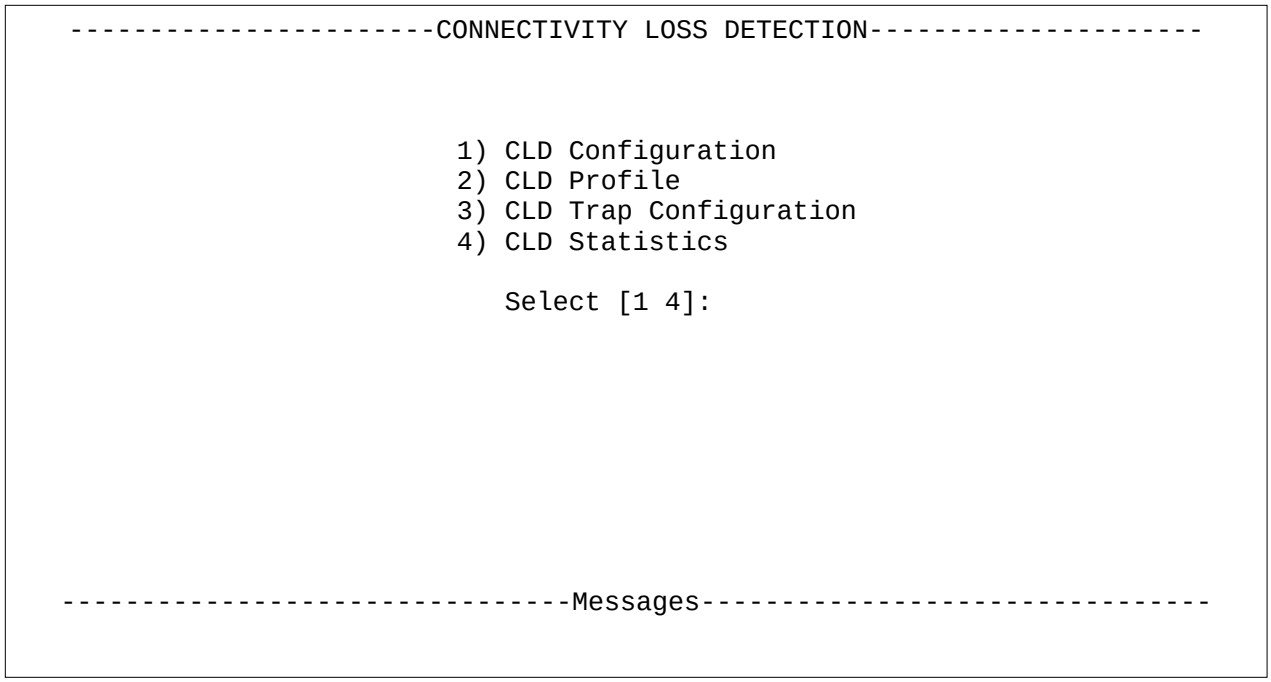

Figure 4-30. N525 Connectivity Loss Detection Screen

Note: The CLD and CLF functions take place in the remote N525 and are managed through the SideBand management channel.

For information on configuring CLD and CLF, see the *N525 Ethernet Termination Service Unit User Manual*.

4.7 Link Status Screen

Use the Link Status screen to view the current link conditions on the L351. See Figure 4-31. To view link status, follow these steps:

1. From the Main Menu, type 3, Link Status, and press <Enter>. The Link Status screen appears.
2. When you finish checking the Link Status, press <Esc> to return to the Main Menu.

```
-----------------------------LINK STATUS------------------------------
                            Local                    Remote 9145
Chassis                     Standalone
Slot                        N/A

User Port                   Link Down                Link Down
Extension Port              Link Up                  Link Up

SFP Status:
   User SFP Rx Power        N/A                      N/A
   User SFP Tx Power        N/A                      N/A
   Extension SFP Rx Power   N/A                      N/A
   Extension SFP Tx Power   N/A                      N/A

   Link Loss From Local Ext Tx To Remote Ext Rx      N/A
   Link Loss From Remote Ext Tx To Local Ext Rx      N/A

                 Press ESC to return to previous screen
-------------------------------Messages-------------------------------
```

Figure 4-31. Link Status Screen

4.8 System Alarms

Use the System Alarms screen to view alarms and faults on the L351. See Figure 4-32. To view alarm status:

1. From the Main Menu, type 4, System Alarms, and press <Enter>. The System Alarms screen appears.
2. When you finish checking the Alarm status, press <Esc> to return to the Main Menu.

```
-------------------------------SYSTEM ALARMS-------------------------
                              Local                    Remote 9145

 Configuration Errors         No                       No
 User Port                    *** Down ***             *** Down ***
 Extension Port               Up                       Up
 User Port Remote Fault       N/A                      N/A
 Ext Port Remote Fault        No                       No
 Link Loss Echo               No
 Link Loss Fwd Ext->User      No                       No
 Link Loss Fwd User->Ext      No                       No
 Side Band Mgmt Channel       OK                       OK
 User SFP Transmitter         N/A                      N/A
 Extension SFP Transmitter    N/A                      N/A
 Chassis Management           N/A
 Alarm Relay Inputs           N/A
 Power Supply Primary         OK                       OK
 Power Supply Secondary       N/A
 Fan                          N/A
 Chassis Temperature          N/A
------------------Hit 'ESC' to return to previous menu---------------
```

Figure 4-32. System Alarms Screen

4.9 Layer 2 Statistics

Use the Layer 2 Statistics screen to view data transfer protocol statistics on the L351. See Figure 4-33. To view layer 2 statistics, follow these steps:

1. From the Main Menu, type 5, Layer 2 Statistics, and press <Enter>. The Layer 2 Statistics screen appears.
2. To reset the counters, press <Ctrl-R>.
3. To view additional statisctics for the remote module, press <Tab>. At that screen, you can access remote RMON statistics; tyep 2 and press <Enter>.
4. When you finish checking the statistics, press <Esc> to return to the Main Menu.

```
----------------------LAYER 2 STATISTICS (CURRENT)----------------------

                           Local          Local      Remote 9145    Remote 9145
                         User Port      Ext Port       Ext Port      User Port
 Link State             ** DOWN **         UP             UP        ** DOWN **
 Speed/Duplex               N/A        100M/FULL      100M/FULL         N/A
 Frames Sent                  0              0         183920              0
 Frames Rcvd                  0         183921              0              0
 Bytes Sent                   0              0       11770880              0
 Bytes Rcvd                   0       11770944              0              0
 Undersize < 64               0              0              0              0
 Oversize > 10000             0              0              0              0
 Frames > 1518                0              0              0              0
 Frames Sent Rate           0/s            0/s
 Frames Rcvd Rate           0/s            1/s

 Last Counter Reset: 2 days 03:05:41

        Select [(N) Remote RMON Statistics, (M) More Remote Statistics,
     (E) Error Counters, (CTRL-T) Raw Counters, (CTRL-R) Reset Counters]:

-------------------Hit 'ESC' to return to previous menu---------------
```

Figure 4-33. Layer 2 Statistics Screen

4.10 Utilities

Use the Utilities screen to set the time and date, update modem, SLIP, or PPP parameters, or to run the diagnostic PING. See Figure 4-34 and Table 4-12. Options 5 through 9 are available only when the L351 is in a standalone enclosure. To access the Utilities screen, follow these steps:

1. From the Main Menu, type 6, Utilities, and press <Enter>. The Utilities menu appears.
2. To return to the Main Menu, press <Esc>.

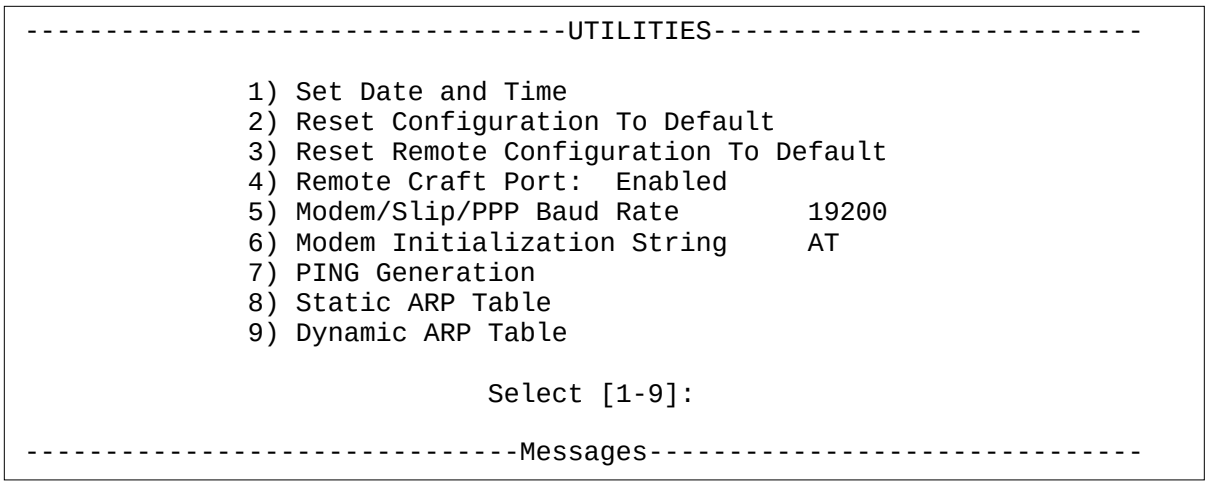

Figure 4-34. Utilities Menu Screen

Table 4-12. Utilities Menu Options

Item	Definition
1. Set Date and Time	Change the time and date information for the modem if needed; if in a chassis with a DMM, the DMM date and time overrides the L351
2. Reset Configuration To Default	Restores all configurable settings to the defaults except for: date and time; password; BOOTP; Telnet timeout
3. Reset Remote Configuration To Default	
4. Remote Craft Port	Enable or disable the console port on the remote module
5. Modem/Slip/PPP Baud Rate	Select the baud rate, 9600, 19200, 38400, 57600, or 115200 bps for the modem/SLIP/PPP serial port
6. Modem Initialization String	The default string is AT
7. PING Generation	Access the PING diagnostics screen
8. Static ARP Table	Set or change specific IP and MAC addresses
9. Dynamic ARP Table	View current IP and MAC addresses

4.10.1 PING Generation

Use the PING Generation screen to test the connection to a specific IP address. See Figure 4-35. To use PING to check a connection, follow these steps:

1. From the Main Menu, type 7, Utilities, and press <Enter>.
2. From the Utilities menu, type 7, PING Generation, and press <Enter>.
3. At the PING menu prompt, set the PING parameters, and press <Enter>.
    - PING response received... indicates a good connection
    - TIMEOUT: Unable to reach [IP address]... indicates a faulty connection.
4. To stop the PING , press <Esc>.

```
-------------------------PING GENERATION-----------------------------

                        1) Ping Address        : 0.0.0.0
                        2) Ping Count          : 0
                        3) Start Pinging

                              Select [1-3]:

-------------------------------Messages------------------------------
```

Figure 4-35. PING Generation Screen

4.10.2 Static ARP Table

Use the Static ARP Table to set specific IP and MAC addresses for up to 10 ports. See Figure 4-36. To use view, set, or remove an address, follow these steps:

1. From the Main Menu, type 7, Utilities, and press <Enter>.
2. From the Utilities menu, type 8, Static ARP Table, and press <Enter>.
3. At the prompt, type 1 to add an entry or 2 to remove an entry, and follow the prompts.
4. To return to the Utilities menu, press <Esc>.

```
-------------------------------STATIC ARP TABLE-----------------------

              IP Address              MAC Address
              ----------              -----------
              172.16.2.7           00-90-37-56-6C-34
              172.16.3.23          00-7C-25-33-57-9C




  Add or Delete an entry (1=Add, 2=Delete from table):


-------------------------------Messages-------------------------------
```

Figure 4-36. Static ARP Table Screen

4.10.3 Dynamic ARP Table

Use the Dynamic ARP Table to view the currently assigned IP and MAC addresses for various ports. See Figure 4-37. To use view an address, follow these steps:

1. From the Main Menu, type 7, Utilities, and press <Enter>.
2. From the Utilities menu, type 9, Dynamic ARP Table, and press <Enter>.
3. To return to the Utilities menu, press <Esc>.

```
-------------------------------DYNAMIC ARP TABLE----------------------

IP Address         MAC Address           IP Address         MAC Address
----------         -----------           ----------         -----------
172.16.2.7       00-90-37-56-6C-34
172.16.3.23      00-7C-25-33-57-9C




                        Press Enter to Delete an entry
```

Figure 4-37. Dynamic ARP Table Screen

4.11 Software Upgrade

Use the Software Upgrade report and menu screen to check the current version of the firmware and upgrade it and the remote L351, if necessary. See Figure 4-38. To access the Software Upgrade screen and check the software version, follow these steps:

1. From the Main Menu, type `7`, Software Upgrade, and press <Enter>. The Software Upgrade screen appears.

2. Record the numbers for the Active and Inactive Firmware for both the local and remote modules.

3. Access the Canoga Perkins Web site, click Downloads, scroll to the L351 file name and compare the version numbers listed there with the version numbers you recorded. The L351 firmware file name is similar to `L3510106.zip`, where L351 indicates the module and 0106 indicates the version number.

Note: The TFTP option is available only for an L351 in a standalone Model 1020.

4. Download the software from the Web site to your local TFTP server.

```
-------------------------------SOFTWARE UPGRADE-----------------------

   Time Since Last Restart 3 days 07:25:16

                           Local                       Remote 9145

   Active Firmware         05.00                       05.00
   Inactive Firmware       84.02                       03.40
   Bootcode                06.00                       06.30

   1)  Software Reset      Reset                       Reset
   2)  Swap Bank & Reset   Swap                        Swap


   3)  Get New File with TFTP


                              Select [1-3]:
```

Figure 4-38. Software Upgrade Screen

Caution: To ensure compatibility when two or more units are connected, you must upgrade all connected units with the same software.

If the firmware on the L351 is outdated, you need to upgrade it. If the L351 is in a chassis or 1030 enclosure within a domain with a DMM, go to the User Manual for the DMM and use that procedure to install the new software. If the L351 is in a Model 1020, follow these steps:

1. TFTP server should be open and running.

2. From the Main Menu, type 7, Software Upgrade, and press <Enter>.

3. At the Software Upgrade menu, type 4, Get New File with TFTP, and press <Enter>.

4. At the prompts, type the IP address for the TFTP server and the File Name.

5. At the prompt, type Y to transfer the file and start the upgrade.

To upgrade a remote unit to the same version of software, follow these steps:

1. From the Main Menu, type 7, Software Upgrade, and press <Enter>.

2. At the Software Upgrade menu, type 3, Copy Software from Source unit to Destination unit, and press <Enter>.

3. At the prompt, select the Source, which is the inactive bank for the local module, then select the Destination, which is the inactive bank for the remote module, and press <Enter>; the upgrade runs automatically.

To run the new software, swap banks, and reset the module, follow these steps:

1. From the Main Menu, type 7, Software Upgrade, and press <Enter>.

2. At the Software Upgrade menu, type 2, Swap Bank, press <Tab> to highlight the Remote column, and press <Enter>.

3. Type 2, Swap Bank, check that the Local column is highlighted, and press <Enter>. Both modules reset and start using the new firmware.

Chapter 5
Maintenance and Troubleshooting

5.1 General Maintenance

Well-maintained components and clearly identified cables help assure optimum system operation. Damaged fiber cables and dirty connectors are a common source of signal loss or attenuation. Single mode and multimode fiber optics are especially sensitive to contamination. Inspect, clean, and test all components to maintain optimum performance.

Note: To avoid damage and signal loss, do not over-tighten or force-fit optical connectors.

- To clean the ferrules and end-face surfaces of male fiber couplings, use a lint-free pad saturated with isopropyl alcohol.
- To clean the female fiber connectors, use canned air.
- To prevent damage and contamination, place protective dust caps on all unused optical connectors.

5.1.1 Manage Cable Links

Plan to manage the cables to ensure trouble-free operation and maintenance tasks.

- Position and secure the fiber optic cables to prevent excessive bends and damage. Follow the guidelines for the bend radius for specific fiber cables.

Note: If no minimum bend radius is specified, the typical long-term, low-stress radius is not less than 15 times the cable diameter (based on Federal Standard FS-1037C).

- Always connect the fiber optic cables in the standard Tx to Rx and Rx to Tx scheme.
- Label each cable near each end with the signal direction, source, and destination to minimize connection errors.

5.1.2 Check Optical Power Levels

To ensure the proper performance levels, measure the fiber link loss, or link attenuation, for all fiber links. Each L351 is shipped with a document that lists the output power for each laser transmitter. To determine link attenuation, use either the L351 Tx source or a hand-held 1310/1550 nm laser source, a fiber optic test jumper cable (with known loss), and an optical power meter.

Note: For accurate results, your test may require a warm-up period of up to 30 minutes before checking power levels.

The transmission laser in the L351 turns on automatically when the chassis receives power.

5.1.3 Measure Transmitter Output Power

To measure the output power, follow these steps:

1. Clean the connectors on the fiber optic test cable, then plug it in to the Tx connector on the L351.

2. Warm up each component for at least 30 minutes.

3. Set the optical power meter to the proper wavelength.

4. Wait two or three minutes for the power reading to stabilize, and then read the output power.

5. Subtract out the test cable loss, then record the power level and compare it to the value on the performance sheet for that particular L351. Measurement tolerance is +/- 0.5 dBm.

Note: When referencing optical power levels with numerical values less than zero, the reading closer to zero is the greater value; for example, -17 dBm is greater than -20 dBm.

6. If the reading is incorrect, repeat the measurement with a different test cable. If the power level is still not within range, call Technical Support.

7. After calculating the link attenuation, subtract that value from the L351 Tx output value to determine the power expected at the remote cable end, which is the input power at the remote receiver.

5.1.4 Measure Receiver Input Power

If you know the link attenuation, skip this section. Otherwise, follow these steps to use the L351 to measure the link attenuation.

1. At the local site, connect the fiber link cable to Tx on the L351.

2. At the remote site, set the optical power meter to the proper wavelength and connect it to the fiber link cable.

3. Record the optical power level and compare it with the sensitivity level listed on the data sheet for the link fiber type.

4. Subtract the remote power level from the value for the transmitter output power at the local site. The result provides the link loss, in dB. The received power level must not be lower than the Rx sensitivity nor greater than the Rx saturation listed in the optical specification for the model of L351 or SFP used.

Note: If you cannot determine the Rx sensitivity, contact Canoga Perkins Technical Support Department for assistance.

5.1.5 Measure Fiber Link Attenuation

Determine and record link attenuation before starting normal link traffic. The attenuation factor identifies potential problems with links that are on the threshold of receiver limitations.

Measure optical fiber links at the shortest wavelength of operation to determine the limiting factor in the loss budget. Each device that transmits to an L351 has a loss budget that is specified by the manufacturer and recorded on a data sheet provided with the equipment. That loss budget must be greater than the total of the measured loss of the fiber link and the attenuation of the L351s.

Use a power meter calibrated for the laser source, then factor in approximately 1 dB for the connector loss from the patch cables between the L351 and the local device. (Each fiber connection can generate 0.5 dB of additional loss.)

Note: Consider this measurement when extending the link at WWDM wavelengths because the shorter wavelengths have a greater loss.

To measure attenuation:

1. Attach the transmit fiber to the local and remote ends of the link.

Note: To avoid damage, do not over-tighten or force-fit the optical connectors.

2. With a properly calibrated optical power meter, measure the optical power on the fiber that will be connected to the Rx connector at one site. Record this reading.

Note: Use either a hand-held power meter or other similar measuring device.

3. Repeat this process at the other site.

5.2 Troubleshooting

This section describes fault conditions and corrective action. The multifunction LEDs and the alarms display all failures.

As a rule, whenever there is a significant signal loss, check the fiber path and the minimum bend radius for potential problems. Remove and inspect the cable connectors, being careful not to damage the fiber end-face surface or the connector housing. Clean all optical connectors before reinstalling them.

5.2.1 LED Indicators

For details on the LED status during a normal start-up, see Chapter 3.

The front panel LEDs show both normal and fault conditions. Additional information about fault conditions appears in the System Alarms and System Status & Configuration screens. To aid troubleshooting, Table 3-1 lists the functions of the front panel LEDs.

5.2.2 New Installation

On new installations, make sure that all steps in Chapter 2 are complete:

1. Check that the STA LED is green.

2. Check that the fiber type (multimode or single mode) matches the L351 optical mode.

3. Make these checks:

   - All fiber cabling is of the same type; do not mix multimode and single mode cables.
   - The fiber optic cable is within the specifications and loss budget of the optic interface module.
   - The line length between the L351 and the remote link does not exceed the allowable loss budget or receiver saturation.
   - All host modules in the link are turned on.
   - All fiber cables are connected Tx to Rx and Rx to Tx.

5.2.3 SW2 and SW3 Settings Ignored

If the L351 was installed in a UCS 1000, UCS 1002 or 1020 and set in the User Interface to software control, it ignores the hardware switch settings. To restore it to hardware control, access the Utilities screen and reset the configuration to default. For details on setting the L351 hardware switches, see Chapter 2.

5.2.4 Problems With Fiber Optics

If the System Alarms screen shows that an Extension Port link is down, inspect and clean the cables and connectors, then replace any damaged fiber. Retest modules after cleaning.

Chapter 6
Specifications

You can also see the specifications for the chassis or standalone enclosure.

6.1 L351 Specifications

Dimensions:	3.0"H x 1.0"W x 9.0"D (7.6 cm x 2.5 cm x 22.8 cm)
Weight:	0.3 lb. (0.136 Kg)
Operating Temperature:	0° to 50° C
Operating Humidity:	Up to 90% (non-condensing)
Power Consumption:	5 VDC 800 mA Maximum
Optical Connectors:	SC

Regulatory Compliance

- ETL, ETLc (UL 60950/CSA C22.2 No. 60950)
- EN 60950
- EN 60825-1
- FCC Part 15B, Class A
- EN 55022
- EN 55024
- EN 61000-3-2
- EN 61000-3-3
- R&TTE Directive (EN 300-386)
- C-Tick (AS/NZS 3548)
- NEBS Level 3 Tested and Certified
- CE Mark

6.2 L351 Models

Model	Fiber Optic Options
L351-1213	100 Mbps 1310 nm MM w/SC, 11 dB
L351-1313	100 Mbps 1310 nm SM w/SC, 10 dB
L351-1333	100 Mbps 1310 nm SM w/SC, 26 dB
L351-1543	100 Mbps 1550 nm SM w/SC, 30 dB
L351-1354	Single Fiber, SC, 100 Mbps 1310 nm SM, Up to 20 km
L351-1564	Single Fiber, SC, 100 Mbps 1550 nm SM, Up to 20 km
L351-1374	Single Fiber, SC, 100 Mbps 1310 nm SM, Up to 40 km
L351-1584	Single Fiber, SC, 100 Mbps 1550 nm SM, Up to 40 km
L351-1070	100 Mbps 1470 nm SM w/SC. 30 dB
L351-1071	100 Mbps 1490 nm SM w/SC, 30 dB
L351-1072	100 Mbps 1510 nm SM w/SC, 30 dB
L351-1073	100 Mbps 1530 nm SM w/SC, 30 dB
L351-1074	100 Mbps 1550 nm SM w /SC, 30 dB
L351-1075	100 Mbps 1570 nm SM w/SC, 30 dB
L351-1076	100 Mbps 1590 nm SM w/SC, 30 dB
L351-1077	100 Mbps 1610 nm SM w/SC, 30 dB

Appendix A
Warranty Information

Current Warranty information is available on-line in the Client Login Area of the Canoga Perkins web site (www.canoga.com) or by contacting Technical Support at 800-360-6642 (voice) or fiber@canoga.com (email).

Appendix B
Acronym and Abbreviation List

BAM	Bus Access Module
CIM	Chassis Interconnect Module
CLD	Connectivity Loss Detection
DMM	Domain Management Module
FPGA	Field Programmable Gate Array
LLE	Link Loss Echo
LLF	Link Loss Forwarding
LNK	Link
Mbps	Megabits per second
MDM	Modem
MMF	Multimode Fiber
PHY	Physical Layer
RMTF	Remote Fault
Rx	Receive signal
SBMC	SideBand Management Channel
SM	Single Mode
SMF	Single Mode Fiber
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
TRM	Terminal
Tx	Transmit signal

CANOGA PERKINS CORPORATION

20600 Prairie Street
Chatsworth, California 91311-6008 USA
Phone: (818) 718-6300 FAX: (818) 718-6312
Website: www.canoga.com
Email: fiber@canoga.com